SComputer veilig,
of computer niet

Onderzoek naar de totstandkoming van computer beveiligingsgedrag

Marike van Dijk

Computer veilig,
of computer niet

Onderzoek naar de totstandkoming van computer beveiligingsgedrag

Afstudeerscriptie voor de opleiding Psychologie
Marike van Dijk, s0082082
Universiteit Twente, Enschede
juni 2007

Afstudeerbegeleiders:
Dr. J.M. Gutteling
Dr. M.W.M. Kuttschreuter

amenvatting

Het aantal internetgebruikers stijgt, de tijd die men online doorbrengt stijgt en mensen downloaden steeds meer. Inherent aan de stijging van de online handelingen, stijgen en evolueren ook de risico's die aan het internetgebruik verbonden zijn. Phishing, Trojans en Spyware zijn voorbeelden van actuele bedreigingen. Aan de hand van een aantal viruspreventieregels wordt onderzocht hoe het computerbeveiligingsgedrag van 184 studenten en medewerkers van de faculteit Gedragswetenschappen aan de Universiteit Twente tot stand komt.

Het computergedrag wordt verklaard door een aantal bestaande modellen. De Sociaal Cognitieve Theorie wordt gebruikt vanwege het reciprocale karakter van de persoons, omgevings-, en gedragseigenschappen.Ook spreekt het model van effectiviteit- en uitkomstverwachtingen, die een plaats krijgen in het onderzoeksmodel. Het Technology Acceptance Model gaat uit van een externe stimulus die achtereenvolgens een cognitieve respons, een affectieve respons en een gedragsmatige respons teweegbrengt. Het onderzoeksmodel kent dezelfde structuur. Het construct aangaande attitude wordt een het onderzoeksmodel toegevoegd. Het model van Compeau en Higgins (1995) beschrijft het construct Computer Self-Efficacy (CSE), die in het onderzoeksmodel als cognitieve respons wordt gezien op een externe stimulus. Niet alleen de CSE, maar ook angst, affect en uitkomstverachtingen worden beschreven als een cognitieve respons hebben alleen invloed op het computergebruik. Hier wordt het construct aangaande ervaring aan toegevoegd. Het model van Marakas, Yi en Johnson (1998) beschrijft constructen die in het onderzoeksmodel terug komen als externe stimuli. De persoonlijkheidseigenschappen, sociale invloed, sekse, leeftijd en controle worden gebruikt.

De risicoperceptie van mensen aangaande de internetrisico's wordt gekoppeld aan de literatuur aangaande het computergebruik. De risicokarakteristieken van Ropeik (2004) worden gebruik in de aanvulling van het onderzoeksmodel. Vertrouwen wordt gezien als een affectieve respons, de waargenomen controle wordt gebruikt als externe stimulus evenals onzekerheid ten opzichte van de computer. De risico-voordeel verhouding van het risico wordt gezien als de verwachting over de uitkomsten van het eindgedrag. Ook worden kinderen beschreven als risicokenmerk. De externe stimuli bestaan uit persoonlijke factoren (Leeftijd, sekse en angst en volharding), de omgeving (verbale persuasie, sociale steun, indirecte ervaring en computerbeheer) en de mate van controle (kinderen, onzekerheid en kwantiteit). De cognitieve respons wordt gemeten door de specifieke computerangst, de Computer- en Internet Self-Efficacy (CISE), de ervaring en de uitkomstverwachtingen. De affectieve respons wordt gemeten door vertrouwen en de atitude. Deze zullen correleren met het eindgedrag, namelijk het computerbeveiligingsgedrag.

De vragenlijsten over attitude (Computer Attitude Scale, Internet Attitude Items), CISE (Computer User Self-Efficacy Scale, Internet Self- Efficacy Scale) en (computer) angst (Computer Anxiety Rating Scale, NEO-PI-R) bestaan al in de literatuur, dus hiervan is gebruik gemaakt. Er is gekozen voor een opbouw in de vragenlijst, waardoor de moeilijkste items als laatste aan bod zullen komen. Dit zijn de items betreffende de angst en volharding en de onzekerheid. Na de persoonlijke en demografische constructen komt het eindgedrag aan

bod, waarna het onderzoeksmodel wordt terug gewerkt. Er is een pilot afgenomen, waarna de verbeterde vragenlijst via www. surveymonkey.com is afgenomen.

De vragenlijst is ingevuld door 184 respondenten. De groep is onderverdeeld in 109 studenten (59,2%) en 75 medewerkers (40,8%). De vragenlijst is ingevuld door 111 vrouwen (60,3%) en 73 mannen (39,7%). De gemiddelde leeftijd is 29,6 jaar. De analyse van de interne consistentie wijst uit, dat met name de angst en volharding (α= .76), de computerangst (α= .70) en de CISE (α= .81) bijdragen aan een goed meetinstrument. Het omgevingsconstruct (α= .66), de uitkomstverwachtingen (α= .60), de attitude (α= .68) en het eindgedrag (α= .64) zijn redelijk goed te noemen. Factor analyse wijst uit, dat de mate van controle bestaat uit twee factoren, te weten vertrouwen en kinderen. Voorts blijkt, dat vertrouwen goed correleert met de affectieve responsies en met toegevoegde affectieve items laadt op een enkele factor. De resterende items die de mate van controle beogen te meten kennen een goede Cronbach Alpha (α= .76), maar hebben te weinig respondenten om conclusies te verbinden aan de correlatiecoëfficiënten (N=27). De oorzaak hiervan is, dat er weinig respondenten zijn met kinderen. Het construct aangaande het vertrouwen is net niet redelijk goed (α= .59). De items die de ervaring beogen te meten zijn onbetrouwbaar. Alle positieve antwoorden krijgen 1 punt, alle negatieve 0. Hierdoor ontstaat een coëfficiënt die als indicator zal worden gebruikt.

De angst en volharding, de computerangst, de CISE, de onzekerheid en de attitude zijn voldoende intern consistent om een goede bijdrage te leveren aan de kwaliteit van het meetinstrument. De overige constructen zijn redelijk, behalve de mate van controle en de ervaring. De eerste vanwege de beperkte doelgroep die kinderen heeft en de tweede vanwege slechte items. Over veel constructen kunnen valide conclusies worden getrokken.

Door middel van de Spearman correlatieanalyse blijkt, dat er veel samenhang bestaat tussen de constructen in het model. De persoonlijke –en het omgevingsconstruct (externe stimuli) hangen samen met en de computerangst en uitkomstverwachtingen (cognitieve respons). Hierbij is geen significante correlatie gevonden voor de samenhang tussen de externe stimuli en CISE. Ook is er veel samenhang tussen de cognitieve responsies en de affectieve respons. Er is met name samenhang tussen de computerangts, de CISE, attitude en onzekerheid. Een andere opmerkelijke uitkomst is, dat in tegenstelling tot de literatuur er veel directe samenhang is tussen de constructen en het eindgedrag.

Er kan geconcludeerd worden dat veel gestelde hypotheses kunnen worden bevestigd. CISE en attitude blijken een grote rol te spelen in de totstandkoming van compute-beveiligingsgedrag. Veel constructen correleren met het eindgedrag, degenen die dat niet doen hebben op een indirecte wijze effect op het eindgedrag. CISE hangt samen met onzekerheid, waardoor de vraag ontstaat of onzekerheid geen belangrijk onderdeel is van CISE. In dat geval kan gezegd worden, dat CISE een belangrijk construct is in de perceptie van het internetrisico. De mate van controle vertoont een samenhang vertrouwen, zoals de literatuur voorschrijft. Ook wordt de discussie gevoed hoe de affectieve en cognitieve constructen zich laten onderverdelen. De TAM is niet geheel bevestigd door de correlatie van CISE met het eindgedrag. Het model van Compeau en Higgins kent wel een directe relatie tussen CSE en computergebruik. Alleen heeft affect hier geen belangrijke mediërende functie. Het model van Marakas e.a. is te omvangrijk om te bespreken, maar de centrale rol van CISE is zeker bewezen in dit onderzoek.

Abstract

The amount of internet users increases. The time spent online increases and people download much more information. Inherent to the incease of online transactions, the risks attacht to the internet also increase en evoluate. Phishing, pharming and Trojans are examples of actual threats. At guidance of certain viruspreventionrules is investigated how the computer safety behavior of 184 students and workers at de faculty of Behavioral Sciences at the University of Twente is created and how riskperception can be integrated in a behavioral model. A researchmodel is created based on the Technology Acceptance Model, the Social Cognitive Theory, the theory of Bandura, the model of Compeau and Higgins (1995) and the model of Marakas et.al. (1998). The external factors consist of personal and demografic constructs, a social construct and a controll construct. The cognitive constructs are computeranxiety, computer- and internet self-efficacy (CISE), mastery or computerliteracy and outcome expectancies. The affective responses consist of attitude and trust. These result in internet safety behavior.

Fear and persistence, computeranxiety, CISE, uncertainty and attitude are intern consistent enough to create a valid instrument. The rest of the constructs are reasonably well, besides mastery and controll. The first is constructed in a way that was not good enough. The latter had too few respondens since the respondet needs to have children to answer the questions. Valid conslusions can be made of the constructs.

Spearman correlationanalyses shows, that external constructs, with exception of the controll construct, are significantly related to computeranxiety and outcome expectancies but not to CISE. Outcome expectancies relates to trust as opposed to computeranxiety and CISE. De cognitive responses do correlate with the affective responses, especially the relations between computeranxiety, CISE, attitude and uncertainty. In turn, the affective responses correlate with the endbehavior. Some other striking results are the large amount of significant relations between the contructs en the computer safety behavior.

Most hypotheses can be accepted. Is has been proven, for this group of respondents, that attitude has an important mediating role in the model. However, there are more direct correlations with the computer safety behavior, that are not predicted by the TAM, just like CISE and uncertainty correlate positively and computeranxiety and negative attitude. Thus, computeranxiety has an indirect influence on the computer safety behavior.

It can be concluded that most hypotheses can be confirmed. CISE and attitude appear to have a major role in the implementation of computer safety behavior. Many constructs relate to the endusers' behavior, the ones that do not are indirectly related to computer safety behavior. CISE and uncertainty are very much (negative) related, which raises the question wether CISE should include uncertainty in future research. It can be siad, that CISE is a part of internet riskperception because of it's relation to uncertainty. Control is strongly related to trust, like literature has predicted. The results also feed the discussion of the position of the cognitieve and affective constructs. The TAM is not entirely confirmed, because of the direct relation of CISE and the endusers' behavior. The model of Compeau and Higgins is not entirely confirmed, but the direct relation between CSE and computeruse is confirmed. The model of Marakas et.al. is to large to evaluate, but the central role of CISE is confirmed.

Voorwoord

Iets meer dan een jaar geleden had ik een lang gesprek aangaande een afstudeeropdracht met Jan Gutteling en wist ik meteen dat ik niet verder zou hoeven zoeken. Het was een prettig gesprek en de onderwerpen die in mijn gedachten schoten spraken mij aan en zetten mij aan het denken. Dat het uiteindelijk over computerbeveiligingen risicoperceptie zou gaan had zelfs ik niet kunnen verwachten. Ik wist nog niet eens hoe ik een backup moest maken! Vandaar dat het me intrigeerde hoe anderen het risico´s van het internet ervaarden en wat er de reden van is dat mensen zoals ik simpele regels vaak niet opvolgen.

De opstartfase duurde lang, niet alleen omdat er gewoon vakken gevolgd moesten worden, maar ook omdat het moeilijk was een overzicht te krijgen van de literatuur. Met de reden dat het een actueel onderwerp betreft, was er niet veel beschikbare literatuur en spraken onderzoeken elkaar nogal eens tegen. Dit draagt niet bij aan een goede beeldvorming over het onderwerp. Ik wist dat ik deze fase van het afstuderen zelf zou moeten doen en in november begon ik eindelijk een intern overzicht te krijgen van de stof.

Aan het einde van januari en het begin van februari is de vragenlijst afgenomen. Dit was erg leuk om te doen en de respons was tot mijn grote vreugde goed. Het analyseren van de resultaten was nagenoeg nieuw voor mij en hier bleek ik inderdaad wat ondersteuning nodig te hebben. Gelukkig voor mij, kon ik enorm steunen op Jan en Margot. Ik heb het gevoel dat ik in die weken meer heb geleerd dan in een half jaar statistiek! Van de terugkoppeling op de literatuur heb ik geleerd hoe belangrijk het is om gestructureerd te werken. Dit zal ongetwijfeld in de toekomst zeer van pas komen.

Zo leest u, dat het afstudeerproces voor mij een bijzonder leerzame periode is geweest. De verantwoordelijken hiervoor wil ik graag noemen.

Allereerst wil ik Jan Gutteling en Margot Kuttschreuter heel erg bedanken. Ik ben geheel onbevangen in het project gestapt en heb me laten leiden. Bewust heb ik geen andere scripties gelezen, omdat ik zelf tot een objectief product wilde komen en niet me niet wilde laten beïnvloeden door anderen. Mede hierdoor had ik geen idee hoe ik de literatuur zou moeten ordenen, de statistiek moest toepassen en tot een goed product moest komen. En toch ben ik nooit onzeker geweest over de voortgang van het project. Waar je vaak hoort dat het afstuderen een vervelend gedeelte is van de studie en dat het voor velen een zware verplichting is, heb ik het dankzij jullie eigenlijk als een leuk project beschouwd!

Mijn ouders verdienen veel dank en lof voor hun onvoorwaardelijk steun! Dankzij jullie aanmoediging heb ik het doorstuderen doorgezet. Dankzij jullie, had ik hier nu niet gestaan. Het is niet te verwoorden hoe goed het is om jullie achter me te hebben staan!

Uiteraard noem ik Roel in mijn dankwoordje, omdat hij ook altijd meer dan ik heel sterk het vertrouwen heeft gehad in mij. Je positivisme en relativeringsvermogen heeft me erg goed gedaan in sommige tijden.

Als laatste wil ik alle vrienden en vriendinnen en speciaal Henry Bruel noemen voor het invullen van vragenlijsten en al het corrigeren. Hulde!!

Marike van Dijk
Enschede, 8 juni 2007

Inhoudsopgave **blz. 5**

Hoofdstuk 1 Theorie **blz. 7**
1.1 Introductie blz. 7
1.1.1 Phishing blz. 8
1.1.2 Spyware blz. 9
1.1.3 Trojan Horse blz. 9
1.1.4 Vooruitblik blz. 11
1.2 Computergedrag blz. 11
1.2.1 Sociaal Cognitieve Theorie (SCT) blz. 11
1.2.2 Technology Acceptance Model (TAM) blz. 13
1.2.3 Computer Self-Efficacy blz. 15
1.2.4 Model van Marakas, Yi en Johnson (1998) blz. 19
1.3 Risicoperceptie blz. 22
1.3.1 Mentale informatieverwerkingsstrategieën blz. 23
1.3.2 Risicokarakteristieken blz. 24
1.4 Onderzoeksmodel en probleemstelling blz. 29

Hoofdstuk 2 Methoden van onderzoek **blz. 34**
2.1 Ontwerp blz. 34
2.2 Operationalisering blz. 34
2.2.1 Externe stimuli blz. 35
2.2.2 Cognitieve respons blz. 36
2.2.3 Affectieve respons blz. 37
2.2.4 Gedragsrespons blz. 37
2.3 Pilot blz. 37
2.4 Deelname blz. 38
2.5 Analyse van de interne consistentie blz. 39
2.5.1 Externe stimuli blz. 39
2.5.2 Cognitieve stimuli blz. 41
2.5.3 Affectieve stimuli blz. 42
2.5.4 Gedragsrespons blz. 43

Hoofdstuk 3 **blz. 44**
3.1 Hypothesetoetsing blz. 44

Hoofdstuk 4 **blz. 52**
4.1 Deelname en kwaliteit blz. 52
4.2 Conclusies correlatieanalyse blz. 53
4.2.1 Persoonlijk construct blz. 54
4.2.2 Omgevingsconstruct blz. 55
4.2.3 Mate van Controle blz. 56
4.2.4 Computerangst blz. 56
4.2.5 CISE blz. 57
4.2.6 Ervaring blz. 58

4.2.7 Uitkomstverachtingen blz. 59
4.2.8 Attitude blz. 60
4.2.9 Vertrouwen blz. 60
4.2.10 Onzekerheid blz. 61
4.2.11 Computerbeveiligingsgedrag blz. 61

Referencies **blz. 62**

Bijlagen **blz.**
Bijlage I Onderzoeksmodel Marakas e.a. blz. 66
Bijlage II Literatuuruitkomsten blz. 67
Bijlage III Vragenlijst blz. 68
Bijlage IV Frequenties blz. 83

Figuren en tabellen
Figuur 1.1 Model van Bandura blz. 12
Figuur 1.2 Technology Acceptance Model blz. 15
Figuur 1.3 Model van Compeau en Higgens blz. 16
Figuur 1.4 Zesfactorenmodel computerangst blz. 18
Figuur 1.5 Model van on-line vertrouwen blz. 26
Figuur 1.6 Onderzoeksmodel blz. 33

Tabel 2.1 Demografische gegevens respondentengroep blz. 38
Tabel 2.2 Cronback alpha, gemiddelde, N en betreffende items blz. 39
Tabel 2.3 Factoren angst en volharding blz. 40
Tabel 2.4 Construct Mate van Controle blz. 41
Tabel 2.5 Items van "Attitude"en "Onzekerheid" blz. 42
Tabel 2.6 Betreffende gemiddelden, N en betreffende items affectieve construsten blz. 42

Tabel 3.1 Correlatietabel constructen blz. 44
Tabel 3.2 Correlaties externe stimuli en cognitieve respons blz. 45
Tabel 3.4 Pearson correlatie van computerbeheer blz. 49
Figuur 3.1 Significante correlaties onderzoeksmodel blz. 50
Figuur 3.2 Model van significante relaties blz. 51

Hoofdstuk 1 Theorie

In dit hoofdstuk wordt allereerst het te onderzoeken probleem verklaard. Wat zijn computervirussen precies en hoe zijn te tegen te gaan? In paragraaf 1.1 vindt u het antwoord op deze vragen. In paragraaf 1.2 zal de literatuur over het computergedrag uiteengezet worden. Gedragsmodellen en vele andere onderzoeksresultaten komen hier aan bod. Hetzelfde wordt voor de risicoperceptie vermeld in paragraaf 1.3. Na de literatuurverantwoording kan in paragraaf 1.4 een opzet voor het verdere onderzoek worden gemaakt. Aan de hand van de theorie en de hypothesse wordt in figuur 1.6 het onderzoeksmodel gepresenteerd. Wanneer er wordt gesproken over een Personal Computer (PC) in deze scriptie wordt daarmee elke computer bedoeld die aangesloten is op het internet.

1.1 Introductie

Het internet heeft in een zeer korte tijd een steeds omvangrijkere functie gekregen in onze samenleving. Tegenwoordig wordt de computer gebruikt voor allerlei dagelijkse activiteiten, zoals bankieren, boodschappen doen, socializen, werk en ter ontspanning (Hinde, 2001). Van alle huishoudens heeft 64% een computer met internet. Van de ondervraagden heeft 73% thuis een computer met internet. Het aantal internetgebruikers stijgt, het aantal uren dat men op het internet doorbrengt stijgt en mensen downloaden en bestellen steeds meer via internet (CBS, 2006). Ook grote organisaties maken veelvuldig gebruik van het internet, waarbij de nadruk vooral ligt op een snelle informatievergaring en –uitwisseling. Ook informatieopslag op het internet gebeurt veelvuldig. Daarnaast maken steeds meer bedrijven gebruik van het internet voor de in- en verkoop van producten. Particulier dient de computer ook veelvuldig ter ontspanning door het spelen van (online) spelletjes, het bloggen of het leggen van contacten via bijvoorbeeld forums.

Er zijn talrijke voordelen te noemen die spreken voor het gebruik van de computer en het internet: het is snel, efficiënt en toegankelijk. Er zijn echter ook nadelen te noemen van het internet, zoals met name de grote risico's die men mogelijk loopt. De risico's van het internet evolueren in een dusdanig tempo, dat het voor providers en andere beschermers tegen het digitale geweld een bijna onmogelijke opgave is om het bij te houden. Het internet en de computers verbeteren zich in hoog tempo, maar de virussen worden in een evenredig tempo slimmer. Mensen weten vaak niet hoe om te gaan met de computer, hetgeen resulteert in het in gevaar brengen van vertrouwelijke informatie. De afgelopen maanden lezen we regelmatig over de fouten die met computermateriaal worden gemaakt. De officier van Justitie die informatie 'op straat zet', de nietsvermoedende defensie- ambtenaar wiens computer wordt leeggehaald. In de Volkskrant van 5 april 2006 is te lezen dat duizenden Word-documenten, wachtwoorden en belastingaangiften uit andermans computer kunnen worden gehaald via online uitwisseldiensten als Kazaa en Limewire. In een artikel in de NRC Next van 20 april 2006 verklaart ook hoogleraar Roos Lindgren (UvA), dat Nederlanders op dit moment onvoldoende bewust zijn van de gevaren van het internet.

Iedereen die zich onbeschermd op het internet begeeft is vatbaar voor virussen.Virussen zijn gevaarlijk vanwege de mogelijkheid om zich aan een ander programma te binden en er zo voor te zorgen dat dit programma ook een virus wordt. Een virus kan zich op deze manier door een computer of netwerk verspreiden en steeds meer programma's besmetten (Cohen, 1984). De definitie van Microsoft luidt: "computervirussen zijn softwareprogramma's die ontworpen zijn voor het opzettelijk verstoren van de computer, bestanden, of het verstoren van data, het verwijderen van data of het verspreiden van data naar andere computers en over het internet, waardoor alles trager wordt en waarbij het andere procesproblemen veroorzaakt" (Microsoft , 2005). Op deze manier kunnen computers besmet worden die belangrijke informatie bevatten. Deze informatie kan gemanipuleerd worden of de computers of het netwerk kunnen in hun geheel uitvallen. De verloren productiviteit en het herstel aan bestanden is voor veel organisaties en instellingen zeer kostbaar. Het "Melissa-virus" infecteerde bijvoorbeeld het Word-document dat werd geopend en het veranderde de settings van de computer. Om zichzelf verder te verspreiden gebruikte het virus het Outlook-adresboek om het virus verder te sturen (de Vries, 2000). In een aantal dagen is het dus mogelijk om voor miljoenen euro's of dollars aan schade te veroorzaken.

Het doel van de hackers is in de loop der tijd veranderd. De intentie van virusmakers en hackers is verschoven van het verkrijgen van naamsbekendheid naar het opzettelijk toebrengen van economische en technologische schade (de Vries, 2000). De meest recente gevaren, zoals phishing (zie 1.1) worden gebruikt voor persoonlijk gewin. De oplichter verkrijgt vaak persoonlijke gegevens, waarmee geld of informatie wordt gewonnen. De virusverspreider kan de computer van een ander beheren zonder dat de ander zich hiervan bewust is. Er wordt gesuggereerd, dat de gevolgen in de toekomst kunnen verergeren, doordat computers steeds meer verbonden zijn met het behouden van mensenlevens. (Personal Computer Magazine, 2006). Hierbij kan bijvoorbeeld gedacht worden aan medische toepassingen. Een ander aspect dat aan verandering onderhevig is, is de computer zelf. Durndell (2002) maakt de lezer duidelijk, dat telefoons met een internetverbinding dezelfde problemen zullen ondervinden als PC's met een internetverbinding en dus beschouwd kunnen worden als minicomputers.

Er zijn dus gegronde redenen om erg bewust om te gaan met het internet. Hieronder zullen een drietal soorten bedreigingen worden toegelicht, met daarna de mogelijke preventiemaatregelen die particulieren en bedrijven kunnen nemen.

1.1.1 Phishing

Dit is een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie van de mensen te ontfutselen. Met een "nepsite" en een e-mail probeert de oplichter persoonlijke gegevens als creditcardnummers, pincode en sofi-nummer te achterhalen. Een voorbeeld hiervan is een mail die men van de bank ontvangt, bijvoorbeeld van de Rabobank. De mail komt overtuigend over, inclusief logo en huisstijl. In de mail staat een link en aan de mensen wordt gevraagd via deze link hun gegevens te verifiëren. Deze link is echter niet verbonden met de Rabobank, maar met een eigen website, lijkend op die van de bank. Op deze manier verkrijgen oplichters persoonlijke informatie van individuelen. De kenmerken van phishing zijn:

- Spoed, dringend en ernstig.

- Men wordt onpersoonlijk aangesproken.
- Er wordt gewerkt met hyperlinks die de persoon moeten doorverwijzen naar de betreffende site, in dit geval dus de site van de oplichter. De link is vaak gecamoufleerd of verschilt nauwelijks van de echte site.
- Soms worden er bestanden meegestuurd, die spyware kunnen bevatten.
- De mail bevat slordige teksten, vaak met spel- en taal fouten. Soms zijn de mails in het Engels, als de dader een buitenlandse onderneming betreft.

(bron: www.xs4all.nl)

Een andere variant op phishing is pharming. Hierbij krijgt de computergebruiker geen mail, maar gaat de gebruiker zelf naar de website. Het juiste adres van een site wordt ingetoetst, maar men wordt omgeleid naar een “nepsite” (Personal Computer Magazine, augustus 2006).

1.1.2 Spyware

Spyware heeft zijn naam verkregen, doordat het spionagesoftware is. Deze software raakt geïnstalleerd op de computer en maakt de computer op deze manier toegankelijk voor derden of verzendt data via het internet. Hierbij gaat het om gevoelige informatie zoals surfgedrag en privacy- en/of bedrijfsgevoelige informatie. Spyware installeert zich ongemerkt op de computer, waardoor sommigen niet in de gaten hebben wat er met de computer en met gegevens uit de computer gebeurt. Er wordt meer SPAM ontvangen en pop-ups en banners komen vaker voor. Er kunnen ook hoge telefoonkosten ontstaan, zeker als er via een inbelverbinding toegang tot het internet plaatsvindt. Vaak gaat een computer trager functioneren of loopt de computer vaker vast als gevolg van spyware. Spyware installeert zich op drie manieren:

- Door “mee te liften” met software.
  Een programma wordt gedownload en geïnstalleerd op de computer. Zonder dat men er erg in heeft, heeft dit programma een spywarefunctie ingebouwd. Populaire gratis software heeft vaak spyware aan boord, zoals Kazaa.
- Door zichzelf te installeren terwijl men een website bezoekt.
  Het installeren kan op de achtergrond gebeuren of men wordt verleid software te installeren, opdat men de website dan beter zou kunnen bekijken. De aangeboden software is vervolgens voorzien van spyware.
- Als onderdeel van software met licentie.
  Men heeft een nieuw softwarepakket, reeds voorzien van spyware, aangeschaft in de winkel. Zo heeft Microsoft sommige functionaliteiten in haar besturingssystemen ingebouwd die bepaalde gegevens aan hen toestuurt bij het gebruik van haar producten (bron: www.xs4all).

1.1.3 Trojan horse

Iedereen die het verhaal van Troje uit de Ilias kent, zal een vermoeden hebben van de werkwijze van dit virus. Het dringt binnen in een computer door zich voor te doen als iets anders. Het doet zich voor alsof het programma iets nuttigs doet, maar als het virus eenmaal binnen is kan het schade toebrengen (Microsoft, 2005). Iemand anders kan criminele

activiteiten vanuit de geïnfecteerde computer verrichten, maar ook veel informatie en programma's in deze computer wissen. Veel Trojans worden met bekende programma's als MSN en Kazaa verspreid. Het downloaden van illegale software en het installeren van een applicatie kan gevaarlijk zijn. Een groot nadeel van Trojans is, dat virusscanners ze niet herkennen. Als door middel van een Trojan de computer wordt aangesloten op een crimineel netwerk is er sprake van een "botnet". Hoe meer computers er aaneengesloten zijn, hoe beter het is voor de crimineel. Deze zal daarom altijd blijven zoeken naar de zwak beveiligde computers (bron: www.xs4all).

Particulieren hebben vaak een computer thuis en hebben geen idee wat de internetgevaren zijn of hoe ze zich moeten beveiligen. Virussen kunnen worden voorkomen door de laatste updates en antivirus- instrumenten te installeren, door steeds alert zijn op recente bedreigingen en door enkele basisregels te volgen wanneer men surft, downloadt en bijlagen opent (Microsoft, 2005). Een goed antivirusprogramma is dus een noodzaak. Dit zijn programma's die virussen opsporen, in quarantaine plaatsen, verwijderen en verdachte documenten tegenhouden. Daarnaast is het belangrijk dat mensen weten wat ze downloaden. De eerder genoemde programma's als Limewire en Kazaa bevatten veel geïnfecteerde bestanden en als een dergelijk programma wordt gedownload zal er spyware of een virus op de PC terechtkomen. De viruspreventieregels luiden als volgt:

1. Nooit een bijvoegsel openen van iemand die niet bekend is of waarover twijfel bestaat (Personal Computer Magazine, 2006).
2. Van een bekende alleen een bijlage openen als de bijlage bekend is. Er kan een virus inzitten waarvan de zender geen wetenschap heeft (www.microsoft.com).
3. De computer beveiligen met een bekend beveiligingsprogramma inclusief een firewall, antivirus, antispam, antitrojan en antispyware en dit programma regelmatig updaten (www.microsoft.com; Personal Computer Magazine, 2006; www.xs4all.nl).
4. Klik nooit op een link in een e-mail of een externe pagina, maar ga via de officiële website naar de locatie (Personal Computer Magazine, 2006).
5. Gebruik geen Outlook, maar een ander e-mail programma (www.xs4all.nl).
6. Maak regelmatig een backup (www.xs4all.nl).
7. Download van zekere sites (www.xs4all.nl).

Ook bedrijven en corporaties worden gewaarschuwd. Peter Wood (2006) beschrijft in zijn artikel hoe eenvoudig het is om 'in te breken' in een bedrijfsnetwerk en op deze manier veel schade toe te brengen. De meest eenvoudige wijze van hacken blijkt een behulpzaam personeelslid te zijn. Met een eenvoudige misleiding via de telefoon wordt soms zeer gevoelige informatie vrijgegeven door het personeel. Werknemers maken vaak gebruik van eenvoudig te achterhalen wachtwoorden en is het voor criminelen eenvoudig om in te loggen op een bedrijfsnetwerk (Woods, 2006). Uit onderzoek blijkt, dat de helft van de Nederlandse bedrijven die internet gebruikten in 2003, schade heeft ondervonden door een virusaanval (CBS, 2005). In recenter onderzoek van het CBS (2006) blijkt, dat tussen 93% en 99% van de bedrijven met computers een totale beveiliging van de ICT-systemen heeft.

Antivirussoftware is de meest gebruikte beveiliging (CBS, 2000). De beveiligingsmaatregelen voor bedrijven zijn hetzelfde als het gaat om het computergedrag. Voor bedrijven is het van groot belang om het gevaar erg serieus te nemen en de medewerkers

hiervan te overtuigen. Ongeveer 30-50% van alle incidenten is te wijten aan gebrekkige beveiliging binnen de organisatie (Johnson, 2006). De werknemers zouden gewezen moeten worden op de strikte geheimhouding van wachtwoorden. Het is van belang, dat er regelmatig van wachtwoord wordt gewisseld. Dit is voor een medewerker soms vervelend, maar voor een digitale inbreker nog meer. De medewerkers moeten erop worden geattendeerd, dat wachtwoorden zorgvuldig gekozen moeten worden. Als laatste dienen bedrijven hun medewerkers erop te wijzen, dat een laptop op een open netwerk vaak onbeveiligd is en derden er dus gewoon informatie vanaf kunnen halen. Hiervoor is namelijk geen virus nodig (Wood, 2006).

1.1.4 Vooruitblik

Phishing, een Trojan Horse en Spyware zijn de bedreigingen die als uitgangspunt worden genomen in dit onderzoek voor het computerbeveiligingsgedrag van de respondenten. In de volgende paragraaf zal het computergedrag worden besproken. Hier worden verschillende modellen zoals onder andere de Sociaal Cognitieve Theorie en het Technology Acceptance Model besproken. In dit onderzoek zal het uiteindelijk te verklaren gedrag de computerbeveiliging betreffen. Hiervoor is niet alleen een meting van computerbeveiligings-gedrag noodzakelijk. Ook de perceptie van de potentiële risico´s van het internet die mensen hebben is van belang. In de derde paragraaf komt deze risicoperceptie aan bod. Er worden een aantal risicokenmerken verklaard die van belang zijn in de perceptie van de internetrisico´s. In paragraaf 1.4 wordt het uiteindelijke onderzoeksmodel gepresenteerd met de bijbehorende hypothesen, waarin de gedrags- en risicodeterminanten worden gecombineerd om tot een uiteindelijk oordeel over het computerbeveiligingsgedrag van de respondenten te komen.

1.2 Computergedrag

De vraag wat mensen ertoe leidt een bepaald computerbeveiligingsgedrag te vertonen is onderwerp geweest in vele studies. Dit heeft geleid tot een beschrijving van vele modellen en theorieën in de literatuur. Deze modellen en theorieën hebben op hun beurt weer veel meer determinanten van het gedrag opgeleverd, die soms door verschillende terminologieën en ontstaanswijze enige overlap vertonen. Hieronder komt als eerste de sociaalcognitieve theorie van Bandura (1977) aan bod. Deze theorie verklaart gedrag op basis van leerervaring en daarbij is de sociale omgeving belangrijk. Vervolgens worden het Technology Acceptance Model (Davis, 1989) en de theorie over Computer Self-efficacy (CSE) besproken. Als laatste zal het model van Marakas (1998) aan bod komen, om te eindigen met een aantal voor dit onderzoek belangrijke factoren die het computerbeveiligingsgedrag bepalen.

1.2.1 Sociaalcognitieve theorie (SCT)

De sociaalcognitieve theorie komt voort uit de leertheoretische benadering van gedrag. De SCT legt de nadruk op de mens als sociaal wezen en op het belang van cognitieve processen zoals motivatie, emotie en actie. De sociale omgeving is belangrijk in deze benadering van de totstandkoming van gedrag (Pervin en John, 1997). Bandura (1977) beschrijft in de SCT dat persoons-, omgevings-, en gedragseigenschappen met elkaar zijn verbonden. Alledrie de aspecten zorgen voor een wederzijdse beïnvloeding van elkaar. De invloed varieert per activiteit, persoon en omgeving (Bandura, 1977).

Omgevingskarakteristieken kunnen demografische kenmerken of organisationele omstandigheden zijn. Bij persoonlijke eigenschappen kan worden gedacht aan affectieve of cognitieve aspecten. Het resultaat van de gezamenlijke eigenschappen is een gedrag dat geëvalueerd wordt, waardoor er een directe of indirecte ervaring ontstaat. Mensen zijn de oorzaak, maar ook het product van hun omgeving (Luszczynska en Schwarzer in: Connor en Norman, 2005). Figuur 1.1 is van toepassing op dit proces:

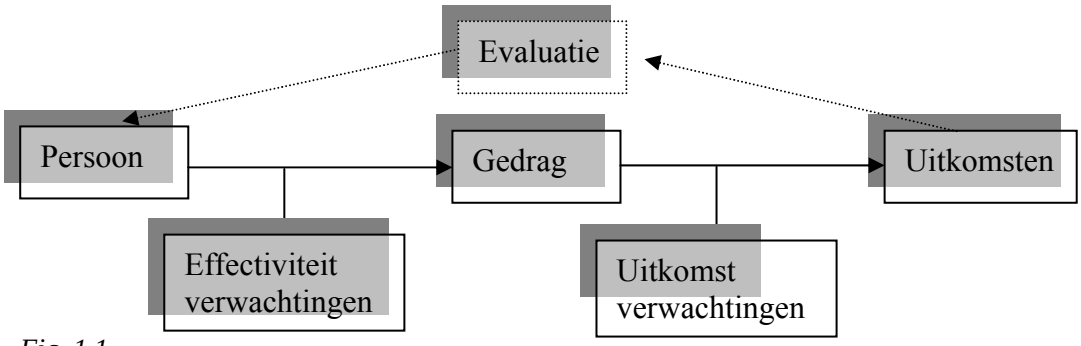


Fig. 1.1
Model van Bandura (1977)

De uitkomst in dit model is niet het daadwerkelijke gedrag, maar een versterking van de (zelf)effectiviteitverwachting, opdat het volgende uitkomsten en uiteindelijk het gedrag verbeterd wordt. Bovenstaande model spreekt ook van de effectiviteitverwachting en de uitkomst verwachting.

Self – efficacy (SE)

De effectiviteitverwachting is de sterkste overtuiging van de eigen effectiviteit. Dit wordt in het model vòòr het gedrag geplaatst, omdat de sterkte van de effectiviteit van groot belang is in de keuze voor een bepaald gedrag. De SE heeft een zeer belangrijke invloed op gedragsintenties (Marakas, e.a., 1998; Davis, 1989, 1993). Mensen die een grote mate van zelfeffectiviteit bezitten zijn meer actief in hun pogingen (Bandura, 1977; Luszczynska en Schwarzer in Connor en Norman, 2005), zeker als men in een eerdere poging heeft gefaald (Igbaria, 1995). Een lage SE wordt geassocieerd met depressiviteit, angst en hulpeloosheid (Luszczynska en Schwarzer in Connor en Norman, 2005). De zelfeffectiviteit kent een viertal bronnen, namelijk succesvolle leerervaring zolang deze maar intern geattribueerd wordt en herhaald kan worden (enactive mastery), modeling of indirecte ervaring, verbale sociale overtuiging en fysiologische en emotionele factoren (Bandura,1977). Hierdoor is zelfeffectiviteit te beschouwen als een dynamisch proces, dat met de komst van nieuwe ervaring weer verandert (Torkzadeh en van Dyke, 2002; Torkzahdeh, e.a., 2006). De theorie is toe te passen op bijvoorbeeld het voetbalveld. Als een persoon een vrije trap kan nemen met als doel te scoren zal hij eerst een oordeel vellen over zijn eigen effectiviteit op dat zekere moment. Als hij een hoge zelfeffectiviteit heeft zal hij de vrije trap nemen. Als hij een lage zelfeffectiviteit heeft zal hij een ander gedrag vertonen, namelijk een ander voor laten gaan.

Uitkomstverwachtingen

De uitkomstverwachting wordt gedefinieerd als de schatting van een individu dat een bepaald gedrag zal leiden tot een bepaalde uitkomt (Bandura, 1977). Het gedrag zal vertoond worden als men gelooft dat het zal leidt tot positieve uitkomstverwachtingen. Deze verwachte consequenties kunnen worden onderverdeeld in fysieke, sociale en zelfevaluatie-uitkomsten (Luszczynska en Schwarzer in Connor en Norman, 2005). Als men bepaald gedrag vertoont zal een verwachting over de uitkomsten volgen. Als de verwachte uitkomsten overeenkomen met de werkelijke uitkomsten zal het gedrag positief worden bekrachtigd en versterkt. Als de uitkomsten niet overeenkomen met de verwachting, wordt dit negatief bekrachtigd. Als de vrije trap is genomen, is de uitkomstverwachting dat er (direct of indirect) wordt gescoord. Als de werkelijke uitkomst slecht uitpakt, zal het gedrag worden meegenomen in een volgende zelfbeoordeling over het gedrag. Een ander zal de beurt krijgen of men zal een andere traptechniek toepassen. Als er daarentegen wel wordt gescoord is de uitkomstverwachting verwezenlijkt en wordt de zelfeffectiviteit hoger bij de volgende zelfbeoordeling. De vrije trap zal de volgende keer met een nog grotere zelfeffectiviteit worden genomen.

De uitkomstverwachtingen worden in het onderzoek van Compeau en Higgins (1995) gesplitst in taakgerichte uitkomsten en persoonlijke uitkomsten. In model 1.4 van computerangst worden de verwachtingen van computerbeveiligingsgedrag gesplitst in positieve en negatieve uitkomsten, waarbij de negatieve uitkomstverwachtingen een rol spelen bij de instandhouding van computerangst en waarbij de positieve uitkomstverwachtingen angst verdrijven. Ook is goed te zien in model 1.4, dat de ervaring (computerkunde) op een indirecte wijze effect heeft op de uitkomstverwachtingen, namelijk via affectie en de fysieke gevolgen. Uitkomstverwachtingen hebben een directe invloed op het computerbeveiligingsgedrag (Compeau en Higgins, 1995). Ook worden de uitkomst-verwachtingen vaak gelijkgesteld aan de waargenomen "usefulness" uit de TAM (Davis 1989; Igbaria,1995). De verwachtingen over de mogelijke consequenties worden op een directe en indirecte beïnvloed door de SE en door computervaardigheden (Shih, 2006).

1.2.2 Technology Acceptance Model

De uitkomstverwachtingen die eerder besproken zijn staan aan de basis van het TAM. Mensen gebruiken de computer als er positieve uitkomsten te verwachten zijn (Davis**,** 1989) Het Technology Acceptance Model (TAM) levert een verklaring voor de acceptatie en het gebruik van technologieën (Davis, 1993). Het TAM wordt gebaseerd op de Theory of Reasoned Action (TRA). Het computerbeveiligingsgedrag wordt bepaald door de gedragsintentie en de gedragsintentie wordt bepaald door de attitude ten opzichte van het gebruik van computers. (Davis, Bagozzi en Warshaw, 1989). De belangrijkste determinanten die de gedragsattitude bepalen zijn de "perceived usefulness ("U")" en de "perceived ease of use ("EOU")". De eerste wordt gedefinieerd als " the degree to which an individual believes that using a particular system would enhance his or her job performance"(Davis, 1993). De laatste wordt gedefinieerd als "the degree to which an individual believes that using a particular system would be free of physical and mental effort"(Davis, 1993). Beide determinanten zijn significant gecorreleerd met de zelfgerapporteerde indicaties van het systeemgebruik. U wordt echter gezien als de primaire determinant en "EOU" wordt gezien als secundaire determinant van de intentie tot gedrag. "EOU" heeft vaak een indirect effect op

de intenties via U (Davis, Bagozzi en Warshaw, 1989; McFarland en Hamilton, 2006)."U" wordt vaak gelijkgesteld aan de uitkomstverwachtingen en "EOU" wordt vaak gelijkgesteld aan SE (Davis 1989; Igbaria,1995).

De TRA kent een subjectieve norm en de TAM niet, wat tevens het grote verschil tussen de twee modellen is. Sociale invloeden spelen wel degelijk een belangrijke rol bij de acceptatie en het gebruik van informatietechnologie (Malhotra en Galetta, 1999). Dit wordt psychologisch attachment genoemd. Deze sociale invloeden hebben effect via de attitude en de gedragsintentie (Malhotra en Galetta, 1999). Een ander verschil is, dat het TAM zich concentreert op waargenomen voordelen, terwijl de TRA het heeft over zowel positieve als negatieve "beliefs" (Horst, Kuttschreuter, Gutteling, 2006). Een schematische voorstelling van het TAM wordt in figuur 1.2 weergegeven.

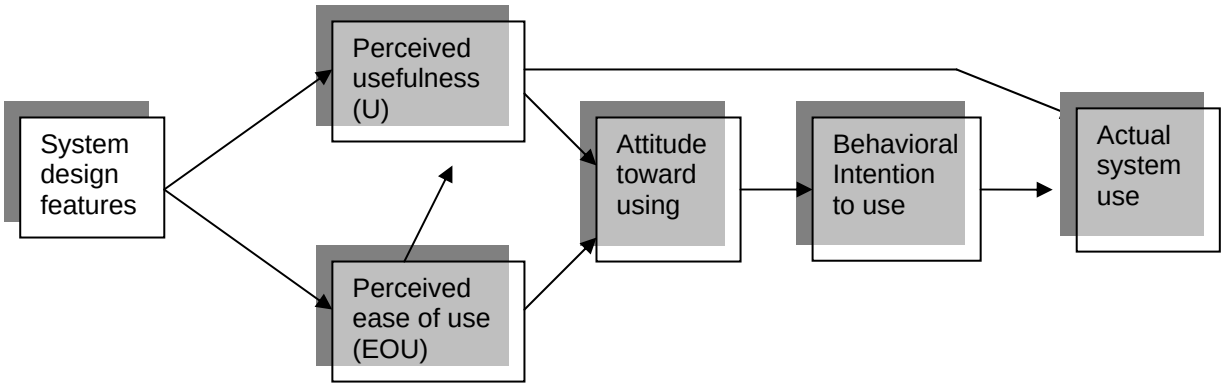


Fig. 1.2
Technology Acceptance Model (Davis, 1993)

Gedragsintentie

De intentie tot computerbeveiligingsgedrag wordt bepaald door de attitude en leidt tot het daadwerkelijke computerbeveiligingsgedrag. Gedragsintentie kan dus gemeten worden, via de computerbeveiligingsattitude. De "U" (waargenomen bruikbaarheid) wordt gezien als de meest significante factor die de intentie beïnvloedt voor het gebruik van Microsoft Word en Excel (Chau, 1996). De attitude ten opzichte van computergebruik correleert significant met de intentie tot gebruik (Dishaw en Strong, 1999), zoals het TAM en de TRA voorschrijven (Connor en Sparks in: Connor en Norman, 2005).. Vanwege de overeenstemming in de literatuur wordt het effect van de gedragsintentie niet gemeten.

Attitude

Zoals in model 1.2 kan worden waargenomen wordt attitude door Davis (1993) als een affectieve respons gezien dat wordt bepaald door de "EOU" (gebruiksgemak) en de "U" (waargenomen bruikbaarheid) betreffende het computerbeveiligingsgedrag. De betekenis van attitude is in de literatuur onderwerp van discussie (Davis, 1989). In een later artikel van Davis (1993) wordt attitude ten opzichte van het technologisch gebruik omschreven als : "the degree of evaluative affect that an individual associates with using the target system in his/her

job". Attitude wordt door de Theorie of Planned Behaviour gezien als een affectieve evaluatie. Torkzadeh en van Dycke (2002) beschrijven attitude als een positieve of negatieve reactie op computers. De positieve of negatieve reactie in de vorm van een goed of slecht gevoel erbij wordt door Beckers en Schmidt (2001) affect genoemd. In hun onderzoek wordt affect gezien als een factor van computerangst. McFarland en Higgins (2006) zien angst als een affectieve staat. Hoewel er geen consensus bestaat in de literatuur over deze constructen zal computerangst in dit onderzoek een cognitieve respons zijn die los staat van CSE en attitude. Mijns inziens is computerangst het gevolg van het denken aan, zien of aanraken van een computer dat al dan geen angstige gedachten teweeg brengt. In het onderzoeksmodel zal computerangst leiden tot een negatieve attitude ten opzichte van de computer. De CSE zal ook een cognitieve verwerking zijn van het beveiligingsprobleem, toegespitst op de zelfovertuiging. Wederom zal er een negatieve correlatie zijn met computerangst en een positieve met attitude, In een later onderzoek van Torkzadeh lijkt hij gebruiksattitude en affect redelijk gelijk te trekken (Torkzadeh, 2006). Desalniettemin zal hier de structuur van de TAM worden aangehouden met attitude als onderdeel van de affectieve respons.

Uit onderzoek is gebleken, dat de attitude significant correleert met het eindgedrag, via de intentie tot het gedrag (Davis, 1993). De literatuur kent een aantal andere bepalende factoren van computerattitude. Geslacht speelt een rol in de vorming van attitude. Mannen hebben een positievere houding ten opzichte van computers dan vrouwen (Durndell en Haag, 2002; Stephens en Creaser, 2001; Schumacher en Morahan-Martin, 2001; Torkzadeh en van Dyke, 2002). Ook correleren ervaring en gemiddelde capaciteiten en computerangst met attitude (Durndell en Haag, 2002). Ook hangt een hoge CSE samen met een positieve attitude (Torkzadeh en van Dyckey, 2002). Een negatieve attitude hangt veel negatiever samen met de CSE dan een positieve attitude.(Torkzadeh, e.a., 2006), maar zowel een hoge als een lage attitude verbetert door training (Torkzadeh en van Dyke, 2002).

1.2.3 Computer Self-efficacy (CSE)

Compeau en Higgins (1995) gaan nog een stuk verder in de theorie. Zij hebben in hun onderzoek de term zelfeffectiviteit toegepast op computergebruik, waaruit de term Computer Zelfeffectiviteit (CSE) is ontstaan. CSE verwijst naar: "het oordeel dat men heeft over de eigen mogelijkheden om een computer te gebruiken" (Compeau en Higgins, 1995). SE heeft in de literatuur van Bandura (1977) drie dimensies, namelijk de omvang (magnitude), de sterkte (strenght) en de mate van generaliseerbaarheid (generelizability). Deze drie dimensies kent CSE ook. De eerste heeft betrekking op de moeilijkheidsgraad van de taak en de eigen capaciteiten om de taak haalbaar te achten, de tweede heeft betrekking op het oordeelsniveau en de derde heeft betrekking op de mate waarin de CSE op persoonlijke of taakspecifieke situaties is betrokken (Compeau en Higgins, 1995). De uitkomsten van dit onderzoek kwamen grotendeels overeen met de aannames die waren gedaan. Computergebruikers met een hoge CSE gebruiken vaker computers, halen meer voldoening uit het gebruik (affect) en ervaren minder angst. Ook affect en angst hadden in dit onderzoek een effect op het gebruik.

CISE (Computer en Internet Self-Efficacy)

Zoals in bovenstaande figuur is te zien heeft CSE een direct effect op het eindgebruik, maar ook een indirect effect via angst en affect. Niet alleen de CSE wordt bepaald door de aanmoediging van anderen (verbale overreding), het computergebruik van anderen

(observatie en indirecte ervaring) en de ondersteuning (assistentie)(Bandura, 1977), maar ook door de uitkomstverwachtingen (Compeau en Higgins, 1995). Een onverwachte conclusie in dit onderzoek is, dat het computergebruik van anderen (observatie en indirecte ervaring) niet van invloed is op de persoonlijke uitkomstverwachtingen, hoewel dit in andere onderzoeken wordt tegengesproken (McFarland en Higgins, 2006; Igbaria, 1995). In dit laatste onderzoek wordt ook bewezen, dat sociale persuasie direct samenhangt met het gedrag en de CSE. Er is echter overeenstemming in de conclusie, dat CSE een direct effect heeft op het gedrag (Compeau en Higgins,1995; McFarland en Higgins, 2006). CSE heeft ook invloed op angst (Wilfong, 2006). Over de relatie van CSE met ervaring schrijven Beckers en Schmidt (2001), dat CSE de verwachting van de ervaring beschrijft.

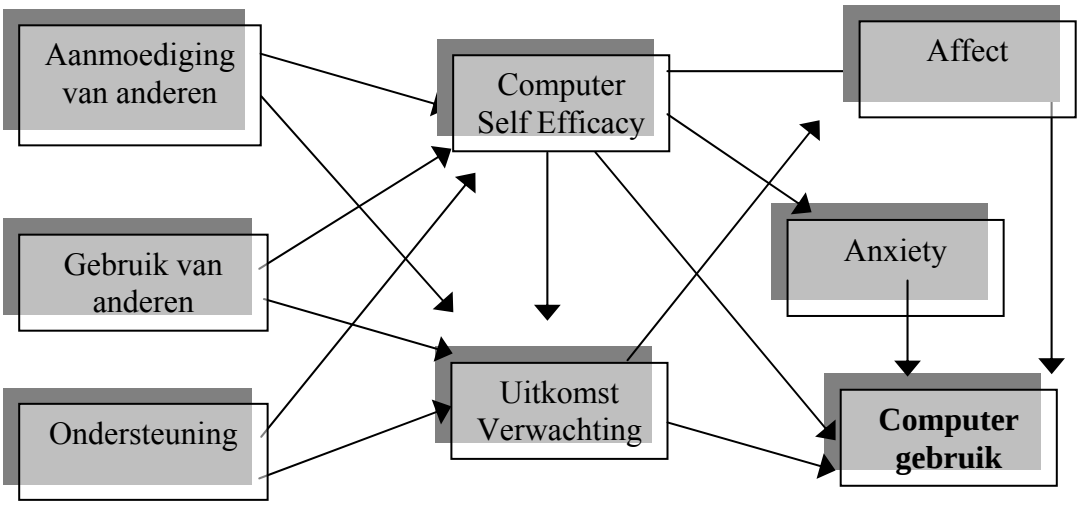


Fig. 1.3
Model van Compeau en Higgins (1995)

Verdere literatuur rondom CSE wijst uit, dat er een algemene vorm van CSE (GCSE = General Computer Self-efficacy) bestaat en een taakspecifieke vorm (ISE= Internet Self-efficacy). De GCSE heeft betrekking op het zelfoordeel betreffende meerdere computer-applicaties. Dit is het product van alle eerder opgedane ervaring en is meestal hetgeen men bedoelt met CSE. Specifieke CSE heeft betrekking op een specifieke taak of applicatie binnen de GSCE (Marakas, e.a., 1998). Een andere specifieke taak is de zelfeffectiviteit in betrekking tot het internet. Dit wordt heel toepasselijk het Internet SE (ISE) genoemd. Het geslacht heeft ook bij deze factor een invloed. Mannen hebben een hogere ISE dan vrouwen, wat grotendeels verklaard kan worden door het verschil in kwantitatieve ervaring (Torkzadeh en van Dyke, 2002): hoe meer men zich op het internet begeeft, hoe hoger de ISE. Dat de mannen uit het onderzoek zich meer op het internet begaven is een andere uitkomst. Torkazadeh e.a. (2006) hebben in hun studie bewezen, dat computertraining de CSE en de ISE verbetert, maar dat computerangst en een negatieve attitude negatief samenhangen met de CSE en de ISE. Ook de interactie tussen angst en attitude beïnvloedt de uitkomsten van de training in de verandering van de CSE, maar niet van de ISE. In het verdere onderzoek worden de CSE en de ISE gecombineerd in het construct dat Computer en Internet Self-Efficacy zal meten (CISE).

Affect

Affect is in het model van Compeau en Higgins (1995) een product van CSE en de uitkomstverwachtingen. Het TAM van Davis (1993) ondersteunt dit doordat de affectieve respons het resultaat is van de cognitieve respons die bestaat uit "U" en "EOU". Het computerbeveiligingsgedrag wordt direct en indirect door affect verantwoord, door de uitkomstverwachtingen en CSE. Voor Beckers en Schmidt (2001) zijn affecten "evaluatieve responsies jegens computers" (voor meerdere definities: zie paragraaf 1.3). De relatie tussen attitude en affect wordt betwist in de literatuur, evenals de relatie tussen angst CSE en attitude/affect. Zo wordt affect in het onderzoek van McFarland en Higgins (2006) gemeten door angst. In dit onderzoek wordt vastgehouden aan de structuur zoals de TAM deze biedt. CISE, computerangst en de uitkomstverwachtingen zijn hierbij cognitieve responsies en attitude een affectieve. Hierover meer op bladzijde 11 en 12.
Ook in de risicoperceptie is affect een belangrijke component. De waarneming van een risico is een oordeel en oordeel heeft een subjectief karakter, ondanks dat men risico's zo objectief mogelijk probeert te benaderen. Deze factor wordt uitgebreider toegelicht in paragraaf 1.3.

Computerangst

Computerangst wordt gedefinieerd als "een negatieve emotionele staat en/of een negatieve cognitie ervaren door een persoon wanneer een persoon de computer gebruikt of wanneer de persoon aan toekomstig gebruik denkt" (Bozionelos, 2001a). De computerangst komt tot uiting in vermijding van gebieden waar computers staan, extreme voorzichtigheid met computers, negatieve opmerkingen over computers en bagatellisering van het nut van computers (Maurer en Simonson, 1984 in: Bozionelos, 2001a).

Uit het bovenstaande model wordt angst veroorzaakt door de CSE (Brosnan, 1998) en veroorzaakt op zijn beurt weer het gedrag (Compeau en Higgins, 1995). In het onderzoek van McFarland en Higgins wordt angst gezien als een affectieve staat en wordt geconcludeerd dat angst negatief correleert met CSE dat vervolgens indirect samenhangt met het gedrag (McFarland en Higgins, 2006; Brosnan, 1998; Igbaria, 1995; Wilfong, 2006). Mensen met een lage mate van computerangst verbeteren hun CSE beter, dan mensen met veel computerangst waarbij het verschil in geslacht geen invloed heeft (Torkzadeh, e.a., 2006). Een andere oorzaak van computerangst die in de literatuur wordt vermeld is een slechte of geringe computerervaring (Wilfong, 2006; Lazar e.a., 2006). Het opdoen van computerervaring is voor angstige mensen ook een zeer effectieve remedie (Bozionelos, 2001b).

Het persoonlijke construct heeft invloed op de angst. Leeftijd speelt een rol, waarbij jongere mensen minder angst kennen. De professionele oriëntatie speelt een rol, waarbij bedrijfskundige en computerkundige studenten minder computerangst hadden (Maurer, 1994). Geslacht kan een verklaring zijn voor een verschil in computerangst. In sommige studies lijkt computerangst meer voor te komen bij vrouwen dan bij mannen (Stephens en Creaser, 2001; Durndell en Haag, 2002; Beckers en Schmidt, 2003), maar in sommige studies ook niet (Brosnan e.a., 1998). De waargenomen controle over computerbeveiligingsgedrag speelt ook een rol in het ontstaan van angst. Door gebrek aan controle kan bepaald gedrag worden vermeden of heeft het een negatief effect op de intentie (Hill, Smith en Mann, 1987). Beckers en Schmidt (2003) hebben ook de noodzaak om met computers te werken onderzocht. Als

iemand uit noodzaak (voor werk bijvoorbeeld) gebruik maakt van een computer heeft dit alleen een indirect effect op de computerangst, via ervaring.

Computerangst kent vele oorzaken en gevolgen. Hierbij is computerangst enerzijds de angst voor een technologie, een angst voor de feitelijke computer. Anderzijds kan de angst ook een negatief affect bij een ervaring betreffen. Ook is angst in aanleg verschillend per individu. De laatste soort angst wordt beschreven als persoonlijkheidstrek. Een negatief affect wordt besproken bij de affectieve responsie, de negatieve ervaring wordt wel bij de cognitieve response behandeld, namelijk door de ervaring dat tot uiting komt in de beheersing. De angst die de feitelijke computer betreft is van toepassing op de cognitieve angst die hier onder computerangst wordt verstaan.

In het model van Maurer wordt computerangst bepaald door de kwantiteit aan ervaring en de persoonlijkheidskarakteristieken. De kwantiteit aan ervaring wordt bepaald door persoonlijkheid, demografische kenmerken en levenskeuzes zoals studierichting (Maurer, 1994). Beckers en Schmidt (2001) onderscheiden zes factoren die een rol spelen bij de totstandkoming of de instandhouding van computerangst, namelijk (1) computerkunde (kennis), (2) zelfeffectiviteit, (3) fysieke prikkeling in de nabijheid van computers, (4) affectieve gevoelens jegens computers, (5) positieve gevoelens over de voordelen van het gebruik van computer voor de maatschappij en (6) negatieve gevoelens over de dehumanisering van computers. De onderzoekers veronderstellen, dat de factoren zich schematisch verhouden zoals in figuur 1.4. Het schema dient als volgt gelezen te worden: computerkunde en zelfeffectiviteit zijn onafhankelijke variabelen voor de fysieke prikkeling die mensen gewaar worden wanneer ze in aanraking komen met computers en hun affectieve gevoelens jegens de computer. Deze factoren beïnvloeden op hun beurt het geloof in computers, hetzij op een positieve, hetzij op een negatieve manier (Beckers en Schmidt, 2001). Uit dit proces komt een mate van computerangst tot stand.

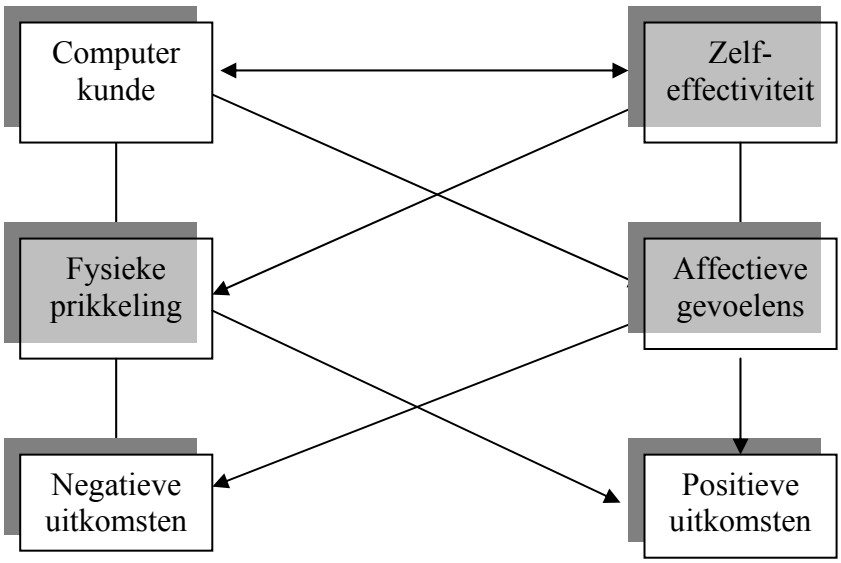


Fig. 1.4
Zes-factorenmodel computerangst (Beckers en Schmidt, 2001)

Ervaring

Hoewel Bandura de grootste pleiter is voor directe ervaring om gedrag te verklaren, wordt deze ervaring niet expliciet getest in het model van Compeau en Higgins. Positieve ervaring (bijvoorbeeld een computertraining) hangt samen met een grotere CSE (Beas en Salanova, 2006; Beckers en Schmidt, 2001; Igbaria, 1995), zeker als het gaat om training in moeilijke en onbekende taken (Hasan, 2003). Eerdere ervaring heeft een positieve invloed op zowel de CSE als het computergedrag (McFarland en Higgins, 2006; Torkzadeh en van Dyke, 2002; Torkzahdeh, e.a., 2006). Andersom geldt ook, dat CSE positief correleert met de computercompetentie (Shih, 2006), hetgeen overeenkomst met het reciprocale karakter van de leertheorieën, zoals die van Bandura (1977). Ervaring hangt in de literatuur negatief samen met computerangst (Wilfong, 2006; Beckers en Schmidt, 2003; Igbaria, 1995). Dit houdt in, dat meer ervaring in relatie staat tot minder computerangst.

Er zijn een aantal oorzaken aan te wijzen die verantwoordelijk zijn voor dit gegeven. De persoonskenmerken hebben invloed op de ervaring. Stephens en Creaser (2001) hebben in hun onderzoek aangetoond, dat sekse een belangrijke factor is die de ervaring bepaalt. Ook leidt computerbezit niet alleen tot een grotere CSE, maat ook tot een grotere ervaring (Cassidy en Eachus**,** 2002; Stephens en Creaser, 2001). Uit onderzoek van Schumacher en Morahan-Martin (2001) blijkt, dat in 1997 meer mannen computers bezaten dan vrouwen. Hier zou dus sprake kunnen zijn van simpelweg meer ervaring door het fysiek meer in staat zijn met een computer te werken. Immers, de ervaring stijgt, naarmate de computer en het internet meer worden gebruikt (Schumacher en Morahan-Martin, 2001). Volgens Hill e.a. (1987) speelt ervaring wel een rol bij het aanleren van computergedrag zoals de SCT voorschrijft, maar heeft ervaring een indirect effect op de gedragsintenties, namelijk via de CSE (Hill, Smith en Mann, 1987; Brosnan, 1998). Torkzahdeh e.a. (2006) voegen eraan toe, dat computertraining meer effectief is voor mensen met een positieve houding naar computers en zo min mogelijk computerangst hebben. Positieve ervaring leidt tot positieve uitkomstverwachtingen (Igbaria, 1995).

1.2.4 Model van Marakas, Yi en Johnson (1998)

Op basis van de modellen die eerder zijn besproken, zijn Marakas e.a. (1998) tot de conclusie gekomen, dat het alle modellen aan een veelheid aan facetten en niveaus ontbreekt (zie bijlage 1). Bandura's voorwaarden voor zelfeffectiviteit zijn duidelijk te zien en ook Marakas e.a. proberen CSE te verklaren. Toch kan volgens hen de CSE vollediger gedefinieerd worden, als het wordt geoperationaliseerd zowel op een algemeen niveau, als op een specifiek applicatieniveau. Deze twee niveaus hebben een reciprocale aard, totdat de taak is aangeleerd. Concreet houdt het verschil in taakspecifieke en algemene applicaties het verschil in tussen een omgevingstoepassing als Windows '95 en op een specifieke toepassing als Word en databases (Marakas e.a., 1998). Bijlage I geeft weer hoe en welke determinanten verklaard worden door deze onderzoekers.

De basis van het model is gestoeld op een positieve relatie tussen de specifieke CSE en de specifieke computeruitvoering. Op basis van evaluatie van de uitvoering vindt een nieuwe beoordeling over de CSE plaats, waardoor de uitvoering verbeterd kan worden. Dit leerproces is heel duidelijk gebaseerd op het model van Bandura (1977) (zie bijlage 1). Zoals is te zien, is het model gericht op een taakspecifiek niveau en specifieke ervaring, die

uitmonden in een vaardigheid. De volgende factoren zijn te onderscheiden: kenmerken van eerdere taken en attribuering van de oorzaak (moeite, vermogen, geluk, taakmoeilijkheid, intellectueel niveau, gezondheid en stemming), taakkarakteristieken (complexiteit, nieuwigheid en moeilijkheid) en situationele ondersteuning (fysieke omgevingsfactoren), waargenomen krachtinspanning en volharding, indirecte ervaring, verbale overreding en feedback, computerangst, emotionele prikkelingen emotioneel gerichte coping, kenmerken van het doel, sekse, leeftijd, tijd, direct volggedrag (motivation to comply) en de professionele oriëntatie. De factoren die van belang zijn voor deze masterthese worden hieronder uitgelicht.

Persoonlijkheidseigenschappen

In het model van Marakas e.a. (1995) wordt volharding genoemd als een directe beïnvloeder van de CSE. Een persoonlijkheidskenmerk zegt vaak ook iets over andere eigenschappen.Volharding is te meten als onderdeel van consciëntieusheid, waarbij doelgerichtheid en zelfdiscipline (NEO-PI-R) ook meegenomen zouden kunnen worden. Er is echter geen literaire verantwoording voor de gedachtegang, dat de eigenschappen bijdragen aan de totstandkoming van CSE, gedrag, evaluatie van dat gedrag en ervaring. Volharding wordt in de studie van Marakas e.a. (1998) gemeten door het aantal afgemaakte taken. In relatie tot computerbeveiligingsgedrag kan volharding een motivationele rol spelen. Dit komt tot uiting in het doorzettingsvermogen in preventief computerbeveiligingsgedrag. Het zou kunnen betekenen, dat een computergebruiker zich aan niet eenmalig aan de regels houdt maar zich altijd aan alle regels houdt. Goldstein e.a. (2002) verklaren wel dat angstige mensen angstiger reageren op nieuwe technologieën.

Sociale invloed

Uit onderzoek blijkt, dat de sociale invloed op het gedrag een belangrijke rol speelt in de uitvoering van computergedrag. Uit het onderzoek van Malhotra en Galetta (1999) blijkt, dat wanneer de sociale invloed een gevoel van onderworpenheid bewerkstelligt, het een negatieve invloed heeft op attitude ten opzichte van het gebruik van een nieuw technologisch systeem. Als de sociale invloed wordt geïdentificeerd en geïnternaliseerd door de gebruiker, zal het een positieve invloed hebben op attitude en het gebruik.

Hoewel het bovenstaande onderzoek van Compeau en Higgins (1995) negatief staat ten opzichte van de verbale persuasie en de sociale ondersteuning, blijkt uit andere onderzoeken, dat er wel degelijk een effect bestaat. De ondersteuning van een organisatie heeft in een onderzoek van Igbaria (1995) een positief effect op de SE en op de U.

Bandura (1977) stelde in zijn theorie dat sociale invloed drieledig is en bestaat uit indirecte ervaring, verbale overreding en feedback (emotioneel of fysiek). Indirecte ervaring komt tot stand door observatie van correct computerbeveiligingsgedrag van bijvoorbeeld een expert, die in feite model staat. Door imitatie worden vaardigheden en regels aangeleerd om het gedrag zo te organiseren, dat er een nieuwe gedragsstructuur is ontstaan. Ook kan een eerder opgedane ervaring worden versterkt of verzwakt (Bandura, 1986). Indirecte ervaring heeft alleen effect als mensen het gedrag inderdaad opvolgen. Hiermee wordt bedoeld, dat mensen met een lage CSE de aanwijzingen van de expert of van een handleiding vaak zullen raadplegen en nauwgezet opvolgen. De Engelse term hiervoor zou "motivation to comply" genoemd kunnen worden. Als mensen hebben leren internetten en leren beveiligen door een cursus is daar eenvoudig achter te komen in een vragenlijst.

Verbale overtuiging kan de CSE vergroten als deze in de vorm van een aanmoediging geschiedt en niet in de vorm van sociale druk (Brosnan, 1998; Marakas, e.a., 1998). Met name na een negatieve evaluatie kan dit belangrijk zijn. Interne en/of externe feedback kan ervoor zorgen dat gedrag beklijft en verbeterd. Het staat vast dat positieve feedback de CSE bevordert. Uit het onderzoek van Compeau en Higgins blijkt, dat modeling of indirecte ervaring niet bijdraagt aan de persoonlijke uitkomstverwachtingen. Het blijkt wel, dat indirecte ervaring een directe invloed heeft op CSE en een indirecte invloed heeft op het computergedrag (Compeau en Higgins, 1995; Brosnan, 1998), hoewel deze indirecte ervaring minder effectief is dan de directe ervaring (mastery) (Igbaria, 1995).
Ook de risicoperceptie die in paragraaf 1.3 besproken is, kent sociale invloeden die de oordeelvorming beïnvloedt. Vrienden, familie, overheid, maar ook evaluatie van het eigen gedrag en de eigen waarneming worden gebruikt om een oordeel te vellen (Slovic, 1987).

Sekse

Uit veel van het voorgaande is al gebleken, dat het geslacht van directe invloed is op de CSE, de ervaring, de computerangst en attitude. Het sekseverschil wordt in de literatuur verklaard door het ondernemende en minder angstige karakter van mannen ten opzichte van computergedrag dan vrouwen. Dit levert meer ervaring op, wat een hogere CSE, meer vaardigheden, minder angst en een positievere attitude oplevert (Schumacher en Morahan-Martin, 2001).

Mannen hebben een hogere CSE dan vrouwen (Cassidy en Eachus, 2002; Durndell en Haag, 2002). Cassidy en Eachus (2002) concluderen op basis van de literatuur dat het verschil tussen mannen en vrouwen stijgt naarmate de taak moeilijker wordt. Hoe complexer de taak, hoe hoger de mannelijke CSE voor deze taak. Ook zijn mannen ervarener en bekender met de taken dan vrouwen. (Cassidy en Eachus, 2002; Durndell en Haag, 2002; Morahan-Martin, 1998; Beckers en Schmidt, 2003; Stephens en Creaser). Vrouwen hebben een hogere mate van computerangst (Durndell en Haag, 2002, Stephens en Creaser, 2001) en hebben een minder positieve attitude jegens het internet dan mannen (Durndell en Haag, 2002; Stephens en Creaser, 2001; Schumacher en Morahan-Martin, 2001). Sekse heeft een indirecte invloed op gedrag, namelijk via de ervaringen (Beckers en Schmidt, 2003). De toename in computergebruik van beide seksen in de loop der jaren heeft wel gezorgd voor een nivellerende werking. (Schumacher en Morahan-Martin, 2001).

Leeftijd

Leeftijd speelt in de meeste studies een rol als het gaat om computergedrag. Er kan sprake van een generatiekloof in het computergebruik, dus ook in het computerbeveiligings-gedrag. Burkhardt en Brass (1990) speculeren over een negatieve correlatie tussen leeftijd en de adoptie van de computertechnologie, hoewel er in hun onderzoek primair onderzoek wordt gedaan naar eventuele veranderde machtsverhoudingen na technologische adoptie. Ondanks dat oudere mensen meer (levens)ervaring hebben, brengt een hogere leeftijd een lagere CSE tot stand. De oorspronkelijke CSE is veel lager in vergelijking met jongere mensen, waardoor er een proces ontstaat waarin cognitie en gedrag betreffende computers daalt (Marakas, e.a., 1998). Bozionelos (2001a) concludeert in een ouder onderzoek, dat Britse studenten die zijn opgegroeid met computers zich ongemakkelijker voelen bij computergebruik dan oudere mensen die later zijn gaan computeren. Een reden hiervoor zou kunnen zijn, dat de

verwachtingen van de studenten hoger zijn dan van de oudere mensen. Jonge mensen kunnen zich afhankelijker voelen. Lazar e.a. (2006) beschrijft echter, dat jongere mensen meer ervaring hebben hebben computers. Een andere constatering dat met leeftijd en computers te maken heeft is het lagere angstniveau van jongere mensen.

Professionele oriëntatie

Studierichting en opleidingsniveau spelen ook een bepalende rol in de mate van CSE. Uit een literatuurstudie van Maurer (1994) blijkt, dat informatica -en bedrijfskundige studenten minder computerangstangst rapporteerden. Een hoog opleidingsniveau duidt op een hogere CSE, door de toename in computerervaring en training (Beas en Salanova, 2006).

Waargenomen Controle

Deze waargenomen mate van controle speelt bij computergedrag een rol en mogelijk bij computerbeveiligingsgedrag. Deze factor wordt echter vaker beschreven in de literatuur over risico en angst. Deze factor wordt uitvoeriger beschreven in paragraaf 1.3.

1.3 Risicoperceptie

Computergebruikers kunnen niet achteloos wat downloaden en surfen zonder op de hoogte te zijn van de risico´s dat hun computergedrag met zich meebrengt. De waarneming van het risico bepaald voor een groot deel de terugkoppeling op het gedrag (zie paragraaf 1.2.1). Als deze opgedane ervaring gebaseerd is op een onjuiste waarneming zal het computergedrag nooit op een juiste manier worden bijgesteld. Dit is wel noodzakelijk om mensen het belang van de eerder genoemde basisregels (zie paragraaf 1.1) duidelijk te maken. De computerbeveiliging kan dus gezien worden als consequentie van de risicoperceptie van een computergebruiker. Het is logisch om de risicoperceptie te bespreken voorafgaande de het computergedrag te bespreken. Hier is echter gekozen voor het omgekeerde, omdat de eerder bespoken modellen een inzicht in het computergedrag geven en dus een beter inzicht in de problematiek bieden.

Risico kent meerdere definities, onder andere: "Risk is a situation or an event where something of human value (including themselves) is at stake and where the outcome is uncertain" (Pidgeon, Kasperson en Slovic, 2003). Risico vormt en wordt gevormd op meerdere niveaus. Individuele, sociale, culturele en politieke niveaus zijn hier voorbeelden van. Op het individuele niveau zijn leeftijd, kwantiteit, capaciteit en ervaring belangrijke risicofactoren. Bij de waarneming van een risico gaat het om een zelfoordeel dat gevormd wordt over het risico. Risico's worden intern niet simpelweg rationeel benaderd, maar ook gevoelsmatig om op die manier een juiste beoordeling van het gevaar te creëren (Ropeik, 2004). Affect speelt een grote rol in de totstandkoming van een oordeel. Affect wordt gedefinieerd als: "de specifieke kwaliteit van goedheid of kwaadheid dat wordt ervaren als een gevoel (bewust of onbewust) en dat een positieve of negatieve kwaliteit van een stimulus afbakent" (Slovic e.a., 2004). In risicoperceptie-onderzoek is het dus belangrijk om te weten te komen hoe mensen zich voelen over een risico. Uit de vorige paragraaf wordt duidelijk, dat affect wordt verdeeld in attitude (Davis, 1993) en vertrouwen.

Er bestaat een onderscheid tussen objectieve en subjectieve risico's. De eerste is risico gebaseerd op wetenschappelijke methoden. De laatste houdt in, de waarneming over deze wetenschappelijke uitkomsten van het gemiddelde individu (Fischhoff, Watson en Hope, 1984). Voor de gemiddelde computergebruiker spelen beiden een rol, maar de verhouding tussen de twee niet duidelijk is. Wel zijn er een aantal cognitieve processen, die de beoordeling van het risico beïnvloeden.

1.3.1 Mentale informatieverwerkingsstrategieën

De risicobeoordeling van computergebruikers kan gebaseerd zijn om statistieken om bepaalde trends en tendensen te ontdekken (Wilkens, 2001; Fischhoff e.a., 1984). Als uit statistieken bijvoorbeeld blijkt, dat er een toename is in geïnfecteerde computers, kunnen mensen zich grote zorgen gaan maken. Dit wordt door Slovic (2000) de wet van de kleine aantallen genoemd.

De oorzaken en gevolgen van een probleem kunnen op verschillende manieren worden geattribueerd. Bij deze verwerking van risico-informatie worden dikwijls fouten gemaakt. Als een computer veelvuldig is geïnfecteerd door virussen, kan de oorzaak verschillend worden geïnterpreteerd. Als de oorzaak door het internet ontstaat kan het gevolg zijn, dat er niet of nauwelijks meer gebruik wordt gemaakt van het internet als preventieve maatregel. Als het probleem intern wordt geattribueerd zal men het eigen computerbeveiligingsgedrag veranderen als preventieve maatregel. De genoemde basisregels zullen dan waarschijnlijk in acht worden genomen.

De "availability heuristic" houdt in, dat mensen zich meer conformeren aan de informatie die makkelijk terug te halen is (Finucane e.a., 2000). Dat kan bijvoorbeeld informatie zijn dat als eerste of als laatste is opgenomen (primacy en recency effect). Als de informatie vaak wordt herhaald zal het eerder kunnen worden teruggehaald. Ook kan de manier waarop informatie is gebracht een rol spelen. Levendige visuele boodschappen worden beter onthouden dan saai geschreven informatie. Ook speelt geheugenorganisatie een rol. Als informatie bijvoorbeeld door een slagzin of een rijm wordt gebracht is het makkelijker terug te halen (Gleitman, 1999). Mensen zijn vaak gevoelig voor voorpaginanieuws. Als er een nieuw virus uitkomt dat op het landelijk nieuws wordt genoemd zal de risicoperceptie erg hoog zijn. Media maken hier dikwijls (bewust of onbewust) gebruik van. Dit blijkt uit onderzoeken betreffende de perceptie van veelgenoemde risico's in de media en nauwelijks genoemde risico's in de media. Hierbij zien mensen een groter risico in de vaak genoemde risico's, terwijl deze feitelijk niet gevaarlijker zijn (Slovic, e.a., 2004).

De "anchoring bias" heeft te maken met het startpunt van de beoordeling. De toegevoegde informatie wordt vergeleken met dit anker. Iemand met een hoog ankerpunt eindigt met een hoge schatting van het risico doordat de informatie bovenop het hoge beginpunt komt. Iemand met een laag beginpunt eindigt met een lage schatting van het risico (Finucane e.a., 2000).

De "hindsight bias" is beschreven door Fischhoff (1974) en houdt in, dat als aan iemand wordt verteld dat een bepaalde gebeurtenis heeft plaatsgevonden, het gevoel ontstaat dat de gebeurtenis voor de persoon onvermijdelijk is geworden.

Bij de "affect heuristic" zijn verschillende personen, objecten en gebeurtenissen in het hoofd gekoppeld aan een bepaalde affectie (Finucane e.a., 2000). De vaak gepubliceerde

oorzaken van risico's zijn meer affectief geladen, waardoor mensen deze informatie snel weer naar boven halen en de beeldvorming laat bepalen door deze argumenten (Slovic, e.a., 2004).

Vanwege de complexiteit van de machine die computer heet, zal ook de mening van een expert een hoge waarde hebben voor de risicoperceptie. Experts worden, zoals al beschreven is, vaak gezien als risicobeoordelaars die worden gekarakteriseerd als objectief, analytisch, wijs en rationeel (Slovic, 1998).

Als laatste moet de waargenomen persoonlijke immuniteit voor een risico worden genoemd. Mensen hebben vaak de neiging om te denken dat het risico van besmetting via internet wel bestaat, maar dat het alleen anderen overkomt. Dit heeft implicaties voor het computerbeveiligingsgedrag.

Deze mentale strategieën in het informatieproces hebben te maken met de cognitieve verwerking van de informatie en doen de risicobeoordeling kleuren, waardoor het niet optimaal overeenstemt met de eigen onderliggende normen en waarden (Slovic, 2000). Veel heuristieken zijn in onderzoek moeilijk te onderzoeken, omdat de manier van informatie-aanbieding niet meer beïnvloed kan worden. Het is niet bekend hoe en welke informatie er aanwezig is met betrekking tot de gevaren van het internet of de technische kennis of de computer zelf. Ook wordt het risico-oordeel van mensen vaak onbewust door bovenstaande heuristieken beïnvloed.

1.3.2 Risicokarakteristieken

De karakteristieken van de perceptie zijn hiervoor beschreven, waaruit blijkt dat er altijd een subjectieve factor meespeelt bij de beoordeling van een risico. Ook wordt de perceptie beïnvloed door de cognitieve informatieverwerkingsprocessen, die zijn beschreven. Er bestaan ook indelingen waarin de perceptie van het risico wordt beïnvloed door kenmerken van het risico zelf.

Vlek (2002) beschrijft elf algemene dimensies van waargenomen riskantheid, te weten de potentiële mate van schadelijkheid en/of dodelijkheid, de fysieke omvang van schade, sociale schade-omvang, tijdsverdeling van schade (acute vs uitgestelde effecten), kans op schade of verlies, beheersbaarheid van de gevolgen (door subject of vertrouwde expert), voorstelbaarheid van (ervaring, vertrouwdheid met) gevolgen, vrijwilligheid van blootstelling (keuzevrijheid), duidelijkheid en belang van de beoogde voordelen, maatschappelijke verdeling van risico's en baten en schadelijke intentionaliteit. De eerste dimensies zijn zeer gericht op risico's en gevaren, die zich fysiek uiten en waarbij er sprake is van een verlies in mensenlevens en aanzienlijke fysieke schade. De laatste dimensies kunnen bruikbaar zijn in het risicoprofiel van het computerbeveiligingsgedrag.

Slovic (1987) heeft in zijn boek een aantal karakteristieken gegeven die uiteindelijk via factoranalyse in drie factoren kunnen worden geplaatst, namelijk "dread", "familiarity"en "exposure". De angst heeft te maken met de mate van controle, catastrofale gevolgen, globaliteit, preventieve controle, fataliteit, bedreiging van toekomstige generaties, moeilijk te verminderen en persoonlijke betrokkenheid. De tweede factor heeft te maken met observeerbaarheid, kennis, snelheid van de gevolgen en de bekendheid. De derde factor gaat over de hoeveelheid mensen die zijn blootgesteld aan het risico (Slovic, 2000).

De karakteristieken van Vlek en Slovic zijn naar mijn idee meer gebaseerd op de gevolgen van een risico. Veel mensen kijken ook naar het gevolg van een risico, maar om het risico te voorkomen zullen mijns inziens toch de oorzaken van een risico besproken moeten worden. In dit onderzoek ligt de nadruk op het computerbeveiligingsgedrag ten opzichte van het risico van besmetting door een virus. Het besmettingsgevaar van computers door het gedrag van de gebruikers is niet levensbedreigend en naar mijn mening zijn deze karakteristieken niet helemaal van toepassing op de problematiek in deze masterthese.

Een andere indeling in risicokarakteristieken is samengesteld door Ropeik (2004) en deze spreekt van vertrouwen (trust), verschrikking (dread), controle, natuurlijk of door de mens gemaakt (natural or man-made), keuze, kinderen, onzekerheid (uncertainty), nieuwigheid (novelty), bewustzijn (awareness), kan het mij overkomen, risico-voordeelverhouding (risk-benefit tradeoff) en catastrofaal of chronisch. Hoewel beide indelingen een overlap hebben is de indeling van Ropeik mijns inziens beter van toepassing op het computerbeveiligingsgedrag. Voor alle indelingen geldt, dat ze veel beter toepasbaar zijn op risico's met meer slachtoffers die ineens fysiek gewond kunnen raken en met een grotere verdeling tussen voor-en tegenstanders. Het internetgevaar is individueler en daarom zijn enkele karakteristieken niet van toepassing. De factor natuurlijk of mensgemaakt is niet van toepassing. Een computer met al zijn voor-en nadelen is vrij duidelijk een mensgemaakt risico. Hoewel de keuzevrijheid wel een rol speelt in het computerbeveiligingsgedrag zal het niet zo uitvoerig worden besproken als de andere karakteristieken. Als mensen voor hun werk gebruik moeten maken van de computer en het internet, is dit gedrag niet geheel vrijwillig. Het afhankelijkheidsgevoel van mensen als het gaat om internet zal misschien een verminderde perceptie van keuze opleveren, maar feitelijk is het internet (nog) geen opgelegd risico. Kan het mij overkomen is een karakteristiek dat inmiddels ietwat achterhaald te noemen is. Zonder gepaste maatregelen overkomt het bijna iedereen. Als mensen geen perceptie hebben van het risico zullen ze geen maatregelen nemen, waardoor een bepaald risico heel groot wordt. Als mensen de gevaren wel zien, zullen ze gepaste maatregelen nemen om de schade te beperken. In deze toepassing is het dus meer een gevolg te noemen dan een oorzaak. Ook het bewustzijn van mensen wordt niet meegenomen. In dit onderzoek ga ik ervan uit dat de respondenten wel bewust zijn van een mogelijke bedreiging, ook al achten ze de kans heel erg klein. Als mensen de gevaren niet zien, is er geen sprake van risicoperceptie. Als laatste wordt het catastrofekenmerk niet meegenomen in dit onderzoek. Er zijn risico's die catastrofale kenmerken hebben. Het eerder genoemde "Melissa-virus" of het "I love you-virus" hebben veel mensen en bedrijven getroffen. Dit kost zeer veel geld, maar geen mensenlevens. Chroniciteit is een kenmerk dat veel in de geneeskunde te horen is als een ziekte onbehandelbaar is. Hoe

Volgens de interpretatie van de risicofactoren bij toepassing op de problematiek, blijven de volgende kenmerken over:

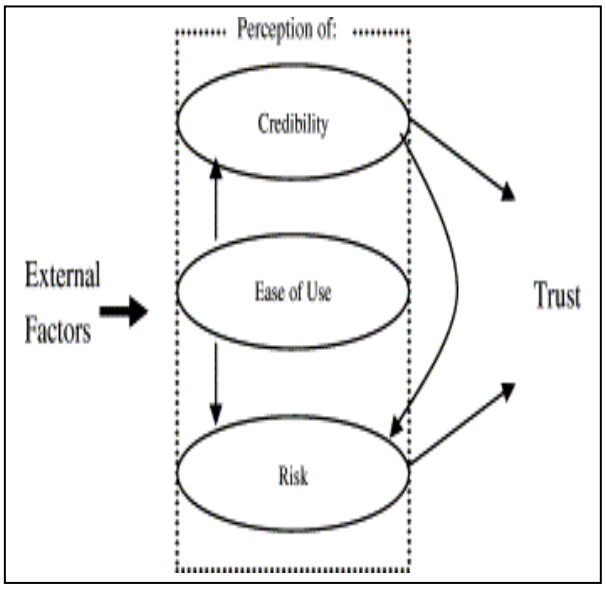
Vertrouwen (trust)

Vertrouwen is altijd aanwezig in een relatie tussen een persoon en een andere persoon, object technologie of situatie (de vertrouwden). Bhattacharya e.a. (1998), geven zes elementen van vertrouwen:

- Vertrouwen bestaat in een onzekere en riskante omgeving.

- Vertrouwen geeft een aspect van voorspelbaarheid weer, het kan gezien worden als een verwachting.
- Elke definitie van vertrouwen moet rekening houden met de sterkte en belangrijkheid van vertrouwen.
- Vertrouwen bestaat in een omgeving van wederkerigheid dat situatie en persoonsspecifiek is.
- Vertrouwen is goed, het gaat over positieve uitkomsten. Hier worden negatieve verwachtingen geïnterpreteerd als sarcasme en/of ironie.

Anderen spreken over vertrouwen als een attitude (Corritore, e.a., 2003; Pidgeon, Kasperson en Slovic, 2003). Deze attitude komt tot stand door risico, gevoeligheid, verwachting, zekerheid en misbruik. Bij computergebruik wordt er een onderscheid gemaakt in off-line trust en on-line trust. Echter, omdat beide veel overeenkomsten hebben en vele off-linebevindingen kunnen worden toegepast in een on-lineomgeving (Corritore e.a., 2003) zal er hierna geen onderscheid meer worden gemaakt in online en offline vertrouwen.
Hoe meer vertrouwen in een positieve uitkomst van het gebruik van het wereldwijde web door middel van surfen en downloaden, hoe minder het waargenomen risico zal zijn. Dit wil niet zeggen dat dit een positieve ontwikkeling is. Zeker met betrekking tot virussen en computerbesmetting is een goede verhouding tussen evrtrouwen en wantrouwen belangrijk. Een model van Corritore e.a. (2003) laat de determinanten zien die bepalend zijn voor het on-line vertrouwen:



Figuur 1.5
Model online vertrouwen (Corritore e.a., 2003)

De gebruikerskarakteristieken van een specifieke situatie betreffen de omgeving, het te vertrouwen object (bijvoorbeeld een website) en de situatie. Ook worden enkele voorbeelden genoemd, namelijk de geneigdheid tot vertrouwen, eerdere ervaring met de handeling en ervaring met het internet. De perceptuele factoren gaan over de geloofwaardigheid, de "EOU" en het risico die geïntegreerd het vertrouwen weergeven. De factor geloofwaardigheid wordt

in vier dimensies verdeeld, namelijk eerlijkheid, expertise (Pidgeon, Kasperson en Slovic, 2003), voorspelbaarheid en reputatie (Corritore, e.a., 2003). Uit verder onderzoek bleek, dat eerlijkheid en expertise dezelfde lading had, omdat in de mening van de participanten de informatie zowel eerlijk als bekwaam moet zijn (Corritore e.a., 2005). De "EOU" wordt beschreven in de TAM (zie paragraaf 1.2) door Davis (1989) en heeft een indirect effect op het vertrouwen. Het risico is de kans op een goede of slechte afloop, waar in de tekst hierboven verder over is uitgewijd. In het artikel van Corritore e.a. (2003) wordt de waargenomen mate van controle aangehaald als het om risico gaat. Het hypothetische geval van totale controle is vertrouwen niet meer nodig. Aangezien het om een hypothetisch geval gaat dat de werkelijkheid op geen enkele wijze weerspiegeld mag duidelijk zijn.

Vrees of angst (dread)

Hoe vreselijker de consequenties lijkt, hoe meer beangstig het computergedrag is (Ropeik, 2004) . De angst van computergebruik heeft een directe en een indirecte implicatie voor de CISE wat intentie en computerbeveiligingsgedrag voor een groot deel bepaald. De kenmerken van angst in relatie tot gedrag en de gevolgen van computerangst worden besproken in paragraaf 1.2.3). De angst is ook een veel beschreven kenmerk van de mate van risico.

(Waargenomen) Controle (control)

Des te groter de waargenomen controle over het gedrag, des te minder bedreigend het is (Ropeik, 2004). Uit de subparagraaf over vertrouwen blijkt, dat hoe meer controle, hoe meer vertrouwen er is. In de perceptie van risico is gebleken, dat vrijwilligheid van deelname aan het computerbeveiligingsgedrag vaak wordt gezien als gecontroleerd gedrag (Slovic, 1987). Er zijn veel mensen die een computer dusdanig ingewikkeld vinden, dat ze denken dat ze er nooit controle over zullen krijgen. Deze mensen zullen de computer proberen te vermijden (Hill, Smith en Mann, 1987). Mannen hebben meer waargenomen controle dan vrouwen op het internet (Torkzadeh en van Dyke, 2002). Goldstein e.a. (2002) hebben in hun onderzoek bewezen, dat bij gebrek aan controle over een nieuwe technologie, mensen angstig worden.

De waargenomen mate van controle wordt in de literatuur verklaard door directe ervaring, omgevingsomstandigheden en heeft zelf invloed op de uitkomst verwachtingen, directe ervaring en CISE. De directe ervaring met het downloaden van een virusscanner of het herkennen van een onveilige bijlage in een e-mail doet het controlegevoel versterken. De omgevingsomstandigheden kunnen te maken hebben met de soort aansluiting. Als men via een modem toegang heeft tot het internet, zal misschien andere downloadgewoonten hebben dan iemand met een snelle draadloze verbinding. Ook brengt het draadloze internet soms op zichzelf al meer risico's met zich mee. Met een draadloos netwerk, zoals tegenwoordig de openbare netwerken in cafés en op stations, dient de laptop goed beveiligd te zijn. Andere mensen kunnen anders direct in de laptop kijken.

Kinderen en een computer in huis kan ook het controlegevoel doen veranderen. Kinderen hebben vaak niet voldoende besef van de gevaren, zijn minder angstig en zijn niet genoeg op de hoogte van de spelregels die genoemd zijn in paragraaf 1.1. Ze zitten bovendien steeds meer achter de computer en steeds meer computers zijn vaker online. Het gevaar dat kinderen op belastende websites terecht komen kan worden uitgefilterd, maar het gevaar dat ze een onschuldig, maar gevaarlijk bestand openen is reëel. Ouders of andere

eindverantwoordelijken voor de computer hebben veel minder controle over de computer. Daarom is de computertijd, de mate van toezicht, de soort verbinding belangrijk voor de risicoperceptie van de eindverantwoordelijke.

De mate van controle heeft op zijn beurt invloed op de uitkomst verwachtingen. Als er een zwakke mate van controle wordt waargenomen, zullen de verwachte consequenties naar beneden worden bijgesteld en vice versa. Ook zal een waargenomen controleverlies invloed hebben op de ervaring en de opgedane kennis over de risico's en de computer-beveiliging. De waargenomen mate van controle zal ook invloed hebben op de CISE. Mensen zullen zichzelf effectiever inschatten als de controle op de handeling groter is.

Kinderen (children)

Kinderen zijn in de literatuur over risicoperceptie een indicatie van ernstigheid (Ropeik, 2004). Risico's waarbij kinderen zijn betrokken lijken risicovoller. Als er door een bepaald gedrag tien kinderen kunnen omkomen wordt dit volgens de literatuur risicovoller beoordeeld ten opzichte van hetzelfde gedrag bij volwassenen. Als deze factor wordt toegepast op een besmettingsrisico via het internet, zal de inhoud van deze factor veranderen. Kinderen zijn niet betrokken bij het gevolg van het risico, maar hebben in deze problematiek van doen met de oorzaak. De kinderen worden hier gezien als een vermindering aan waargenomen mate van controle wat dus in bovenstaande subparagraaf besproken.

Onzekerheid (Uncerainty)

Een grotere onzekerheid heeft meer bescherming als gevolg (Ropeik, 2004). Voor veel mensen is een computer, internet en alle bijbehorende problemen van een dusdanig abstract niveau, dat ze het niet kunnen omvatten. Voor deze mensen is het dus niet voor te stellen wat je jezelf allemaal op de hals kan halen en voelen zich er onzeker door. Als mensen in het geheel onwetend zijn, zullen ze zich naar mijn idee niet erg druk maken om iets. Als mensen echter wel van de bedreiging af weten en de oorzaak van de bedreiging kennen, maar zich verder niet kunnen voorstellen hoe het werkt, kan dat grote onzekerheid met zich meebrengen. Dit leidt volgens Ropeik tot een betere computerbescherming. Mensen die zich onzeker voelen over computers en het internet en niet goed weten hoe de gevaren van het internet zich openbaren en wat ze eraan kunnen doen (bijvoorbeeld de regels naleven) zouden zich veel beter moeten beschermen dan mensen die precies weten waar ze aan toe zijn.

Nieuwigheid (novelty)

Nieuwe risico's lijken beangstigender. Dit construct is lastig om te operationaliseren, omdat tijd relatief is. Het risico dat een computer besmet raakt met virussen via het internet bestaat al een tijd. Anderszijds wordt de computertechnologie wel als een nieuwe technologie beschouwd. De reactie op nieuwigheid van een risico uit zich in angst, dat al in het onderzoeksmodel vermeld staat. Daarnaast is het lastig om deze factor te operationaliseren, omdat naar mijn idee de grens tussen nieuw en niet meer nieuw een erg subjectieve grens is. Het is mogelijk dat de nieuwheid van een risico samenhangt met de onzekerheid, wat misschien voor een volgend onderzoek interessant is.

De risico-voordeel verhouding (risk-benefit tradeoff)

Fischhoff e.a. (1984) heeft het in zijn artikel over het netto-voordeel. Dit is het verschil tussen de voordelen en niet-risicovolle kosten. Het voordeel van computergebruik is bijvoorbeeld (tijd)winst, maar er moet wel een computer worden aangeschaft met een goede internetverbinding. Het netto-voordeel is het verschil tussen de twee. Een ander gegeven is de waarneming dat risico's kleiner lijken naarmate de voordelen stijgen (omgekeerde onderlinge afhankelijkheid) (Alhakami en Slovic, 1994). Dit impliceert ook, dat risico's groter lijken als er weinig voordeel uit te behalen is. Als mensen erg afhankelijk zijn, zijn ze bereid meer risico's te nemen (Fischhoff e.a, 1978; Alhakami en Slovic, 1994). Voorts is een affectieve evaluatie de grootste voorspeller van de risico-voordeelcorrelatie.

De uitkomstverwachtingen die eerder besproken zijn, wordt in dit model gelijkgesteld aan de risico-voordeel verhouding. De reden hiervoor is, dat beide te maken hebben met de verwachte consequenties van een risicogedrag. Als de verwachtte uitkomsten van het risicovolle gedrag positiever zijn dan het niet-risicovolle gedrag, zal men weinig beveiliging toepassen.

1.4 Onderzoeksmodel

De literatuuruitkomsten in bijlage 2 staan aan de basis van het uiteindelijke onderzoeksmodel dat in deze paragraaf beschreven zal worden (zie figuur 1.6). Zowel de TRA als de SCT zijn hierin te herkennen. De TRA is te herkennen aan de structuur van het model, waar duidelijk achtereenvolgend de externe stimulus, de cognitie, het affect en het gedrag worden behandeld. Ook de gedragsintentie en de attitude vinden hun oorsprong in de TRA. De sociaal cognitieve theorie is te herkennen aan het omgevingsconstruct, de uitkomstverwachtingen en de zelfeffectiviteit. Figuur 1.6 laat zien, dat alle factoren leiden tot een optimaal beveiligingsgedrag.

Het uitgangspunt van het model begint bij het persoonlijke construct, het omgevingsconstruct en het gedragsconstruct, zoals de Bandura het bedoeld heeft (figuur 1.1). De persoon, de omgeving en het gedrag worden gevoed door de evaluatie die voortkomt uit eerder gedrag, wat de basis is van een nieuw gedrag. Het model is immers te beschouwen als een proces. Op basis van de TAM kent het model vier hoofdgroepen, namelijk externe (persoonlijke)-, cognitieve-, affectieve- en gedragsdeterminanten.

Hypothese 1

Het persoonlijke construct bestaat uit de leeftijd, het geslacht, de professionele oriëntatie en de angst en volharding. Het persoonlijke construct hangt samen met het omgevingsconstruct, de mate van controle en vertrouwen, de computerangst, de uitkomstverwachtingen en de Computer en Internet Self-Efficacy (CISE).

H1a; Leeftijd, professionele oriëntatie, angst en volharding en geslacht, vertonen een significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.

H1o; Leeftijd, professionele oriëntatie, angst en volharding en geslacht, vertonen geen significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.

Hypothese 2

Het omgevingsconstruct bestaat uit de verbale persuasie, de sociale steun en de indirecte ervaring (modeling), die door Bandura (1977) genoemd worden. Computerbeheer wordt hieraan toegevoegd. Hierbij gaat het om het fysieke computerbeheer en om de internetverbinding. Het omgevingsconstruct hangt positief samen met de computerangst, de CISE, de ervaring en de uitkomstverwachtingen.

H2a: Het omgevingsconstruct, bestaande uit verbale persuasie, sociale steun en indirecte ervaring vertoont een significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.
H2o: Het omgevingsconstruct, bestaande uit verbale persuasie, sociale steun en indirecte ervaring, vertoont geen significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.

Hypothese 3

De laatste van de externe stimuli heeft te maken met de mate van controle en wordt in dit model gezien als het gedragsconstruct. De controle over de beveiliging van de computer hangt af van de eigen onzekerheid ten opzichte van het gevaar van besmetting. Ook spelen kinderen een rol in de controle over de beveiliging van de computer, evenals de kwantiteit van computerbeveiligingsgedrag.

H3a: De mate van waargenomen controle, bestaande uit kinderen, onzekerheid en kwantiteit vertoont een significante samenhang met cognitieve responsies, bestaande uit computerangstangst, CISE, ervaring en uitkomstverwachtingen.
H3o: De mate van waargenomen controle, bestaande uit kinderen, onzekerheid en kwantiteit vertoont geen significante samenhang met de cognitieve responsies, bestaande uit computerangstangst, CISE, ervaring en uitkomstverwachtingen.

Hypothese 4

De cognitieve responsies in dit model zijn computerangst, de CISE, ervaring en de uitkomstverwachtingen. De computerangst wordt naast de drie bovenstaande constructen ook bepaald door de CISE en ervaring. De angst is een bepalende factor voor CISE, het affect (attitude en vertrouwen) en het computerbeveiligingsgedrag zelf. Een indirecte invloed is er voor de ervaring en het computerbeveiligingsgedrag. Het computerangstconstruct heeft te maken met de beleving van het besmettingsgevaar. Angstige mensen nemen het risico waar als een groot gevaar waar men zelf weinig effectief tegen op kan treden. Angstige mensen zullen weinig vertrouwen hebben in het computerbeveiligingsgedrag (indirect ook via CISE) en zullen negatief tegenover staan computergebruik staan. Weinig angstige mensen zien nauwelijks een gevaar waardoor de CISE, attitude en het vertrouwen ten positieve blijft.

H4a: Computerangst vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.
H4o: Computerangst vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.

Hypothese 5

Het zelfoordeel over de eigen effectiviteit in het beveiligen van de computer door het uitvoeren van de regels is een zeer bepalende factor. De CISE heeft een directe invloed op de angst, de ervaring, de uitkomstverwachtingen, het affect (attitude en vertouwen) en het uiteindelijke beveiligingsgedrag. Een directe invloed is er ook op de uitkomstverwachtingen, via de ervaring.

H5a: De Computer en Internet Zelfeffectiviteit (CISE) vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.
H5o: De Computer en Internet Zelfeffectiviteit (CISE) vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.

Hypothese 6

De ervaring of de kennis en competentie en directe ervaring met de computer-beveiligingsregels hangen positief samen met de angst, de CISE, het affect en de uitkomstverwachtingen.

H6a: Ervaring, bestaande uit competentie en ervaring, vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.
H6o: Ervaring, bestaande uit competentie en ervaring, vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.

Hypothese 7

De uitkomstverwachtingen hebben te maken met de inschatting die mensen maken over de consequenties van het computerbeveiligingsgedrag. Het computerbeveiligingsgedrag zal worden uitgevoerd als men gelooft dat het positieve consequenties heeft. In de risicopsychologie wordt dit de risk-benefit wisselwerking genoemd. Fischhoff e.a. (1984) hebben het over een net-benefit, het resultaat van de positieve consequenties minus de negatieve niet-risico consequenties. Het resultaat hiervan hangt samen met het computerbeveiligingsgedrag en op het affect.

H7a: Positieve uitkomstverwachtingen vertonen een significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.
H7o: Positieve uitkomstverwachtingen vertonen geen significante samenhang met de affectieve responsies, bestaande uit attitude en vertrouwen en de gedragsrespons.

Hypothese 8

De affectieve respons bestaat twee constructen, namelijk de mate van vertrouwen en attitude. Het persoonlijke construct heeft een indirecte invloed en alle vier de cognitieve responsies hebben een directe invloed op de affectie. De affectieve constructen hangen samen

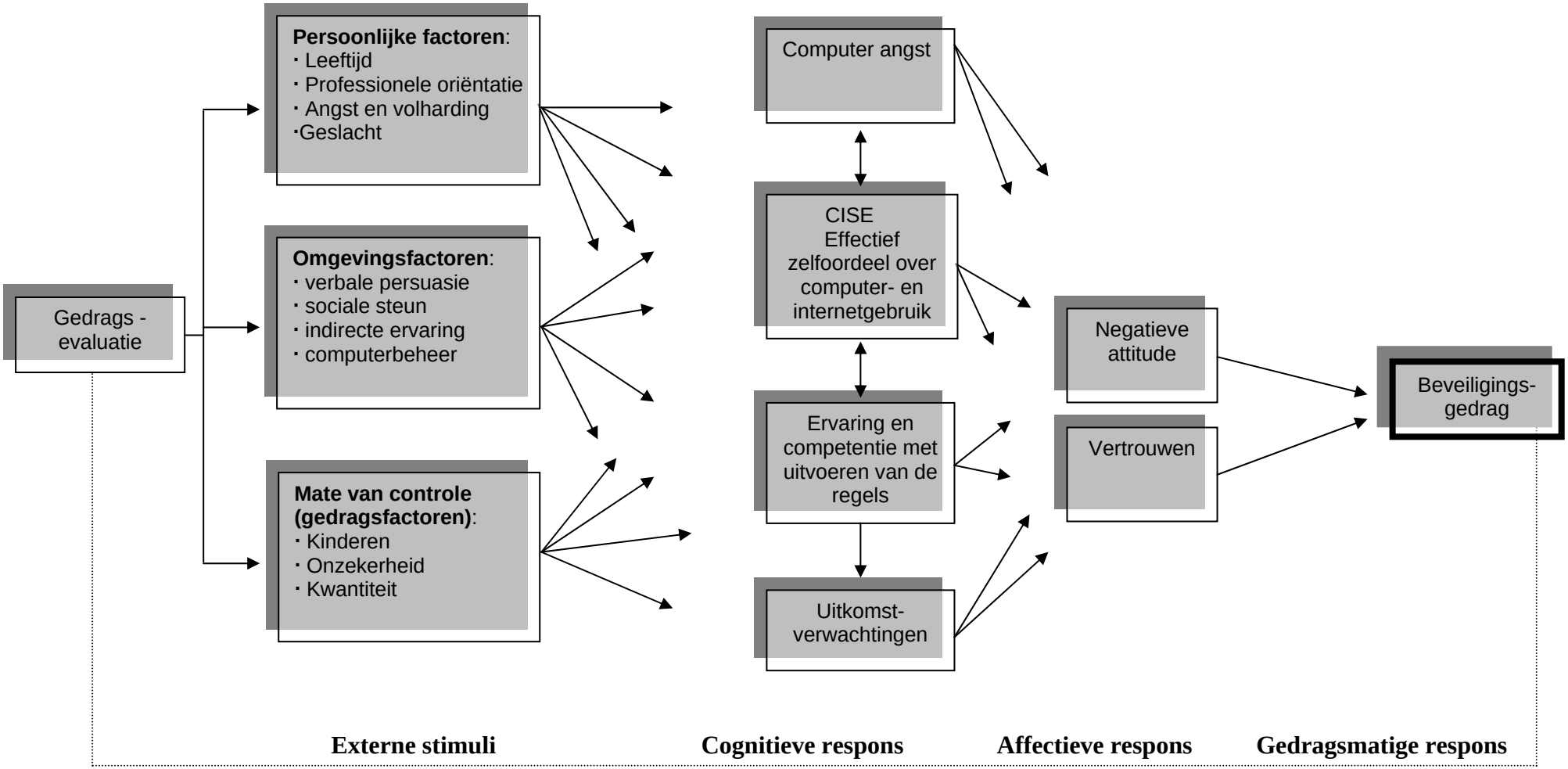
met het eindgedrag. In het onderzoeksmodel is de intentie tot computerbeveiligingsgedrag weggelaten. De gedragsintentie is de motivatie in de vorm van een bewust plan, een beslissing of een zelfinstructie om zich in te spannen om het beoogde computerbeveiligingsgedrag uit te oefenen. De gedragsintentie in dit onderzoek zou bijvoorbeeld het plan om de regels na te leven kunnen zijn. De literatuur voorschrijft echter dat de intentie altijd tot het gedrag en de hypothese zou een overbodige aanname zijn.

H8a: Attitude vertoont een significante samenhang met computerbeveiligingsgedrag.
H8o: Attitude vertoont geen significante samenhang met computerbeveiligingsgedrag.

Hypothese 9

Het vertrouwen zal als affectief construct een samenhang moeten vertonen met het eindgedrag, namelijk het computerbeveiligingsgedrag.

H9a: Vertrouwen vertoont een significante samenhang met computerbeveiligingsgedrag.
H9o: Vertrouwen vertoon geen significante samenhang met computerbeveiligingsgedrag.



Figuur 1.6
Onderzoeksmodel

Hoofdstuk 2 Methoden van onderzoek

In het eerste hoofdstuk is het theoretische kader duidelijk geworden, waarop dit onderzoek is gebaseerd. In paragraaf 1.5 zijn een aantal aannames geformuleerd die in in een onderzoeksmodel zijn geplaatst (zie figuur 1.6). Na dit hoofdstuk is duidelijk op welke wijze de aannames getoetst zullen worden. In paragraaf 2.1 worden het ontwerp van het meetinstrument toegelicht. In paragraaf 2.2 wordt uiteengezet hoe de constructen worden geoperationaliseerd in meetbare items. Hierbij komen eerst de externe stimuli aan bod en vervolgens de cognitieve-, affectieve- en gedragsrespons. Het resultaat van de pilot studie wordt beschreven in paragraaf 2.3. Na de pilot is de definitieve vragenlijst afgenomen bij een doelgroep die in paragraaf 2.4 wordt toegelicht. Om de gewenste resultaten te berekenen moet eerst een conclusie worden gegeven over de betrouwbaarheid van het meetinstrument. Dit komt in hoofdstuk 2.5 aan bod.

2.1 Ontwerp

De hypothesen zullen worden getoetst door middel van een vragenlijst, hetgeen dit onderzoek een survey-onderzoek maakt. Dit type onderzoek is erg nuttig om verbanden tussen variabelen vast te leggen (Dooley, 2001). Hierdoor kunnen uiteindelijk conclusies worden getrokken over de sterkte en de richting van de samenhang tussen de constructen.

De vragenlijst kent verschillende antwoordcategorieën. Bij de meeste items wordt een antwoord in de vorm van een zespunts Likertschaal gegeven. Een neutraal antwoord kan niet worden gegeven, een genuanceerd antwoord is wel mogelijk. Bij de constructie van de vragenlijst is rekening gehouden met een of twee uitvallers per construct. Als een item niet bijdraagt aan een betrouwbaar meetinstrument dan kan het worden weggelaten. De vragenlijst wordt ook afgenomen door enkele mensen die kritisch moeten zijn ten aanzien van de samenstelling. Na de pilot is de vragenlijst afgenomen bij de doelgroep. Met de resultaten is allereerst een betrouwbaarheidsmeting gedaan (zie tabel 2.2).

2.2 Operationalisatie

Vragenlijsten over attitude, CSE (Computer Self-Efficacy, ISE (Internet Self-Efficacy) en computerangst bestaan al in de literatuur.Voor deze verbaal obtrusieve metingen is het inhoudelijk belangrijk, dat zowel de items als de gehele vragenlijst valide en betrouwbaar zijn (Dooley, 2001). Zo mag er bijvoorbeeld geen sprake zijn van dubbelzinnigheden en dubbele ontkenningen. Het item moet begrijpelijk zijn en het is van belang dat er zowel positief als negatief geformuleerde items zijn om een bepaalde antwoordtendentie uit te sluiten. Ook moeten sturende en feitelijke vragen worden uitgesloten. Voor een groot deel van de items wordt een zespunts Likertschaal gebruikt als antwoordmogelijkheid. De proefpersoon moet aangeven of hij/zij het helemaal oneens, oneens, matig oneens, matig eens, eens of helemaal eens is met de stelling. Voor de overige items is een ratioschaal gebruikt. Er is gekozen voor een opbouw in de vragenlijst die de moeilijkst te beantwoorden vragen aan het einde aan bod te laten komen. Zo kan de respondent wennen aan de vraagstelling en zal hij/zij er hopelijk niet mee ophouden als het te moeilijk wordt. In de opbouw van de vragenlijst is ook rekening

gehouden met het onderzoeksmodel. De items die het eindgedrag meten de eersten zijn met een ordinale schaal zijn (items 17a tot en met 17f). Hierna zal het onderzoeksmodel in omgekeerde volgorde worden aangehouden met angst en volharding en computerangst als laatste vragen.

2.2.1 Externe stimuli

De vragenlijst (zie bijlage III) start met een korte instructie waarin duidelijk wordt gemaakt dat de anonimiteit wordt gewaarborgd en dat het enige juiste antwoord een eerlijk antwoord is. Vervolgens wordt ingegaan op demografische items. Niet alleen komen deze items als eerste aan bod in het model, maar hebben de items ook een acclimatiserende functie. De meest persoonlijke items meten de angst als persoonlijkheidseigenschap en volharding (items 28a tot en met 28f). Uit de literatuur blijkt, dat persoonlijkheid in de eigenschap van volharding en angst een indirecte invloed heeft op computerbeveiligingsgedrag (Marakas e.a., 1998). De meting van de mate van persoonlijke angst en volharding is gebaseerd op de N1, N6 en C5 schaal van de NEO-PI-R. De verwoording van de persoonlijkheidsvariabele kan verwarrend zijn. Feitelijk worden angst als persoonlijkheidseigenschap, discipline en volharding geoperationaliseerd. Ook kan het verward worden met het persoonlijke construct (leeftijd, professionele oriëntatie, geslacht en persoonlijkheid). De laatste variabele zal dus angst en volharding genoemd worden.

Het omgevingsconstruct bestaat uit items die betrekking hebben op sociale steun, verbale persuasie en indirecte ervaring (zie paragraaf 1.2). De omgevingsvariabelen met een ordinale schaal zijn de verbale persuasie en indirecte ervaring (items 25a tot en met f). Bij de verbale overtuiging gaat het om de intern geattribueerde aanmoediging en is het van belang dat er onderscheid wordt gemaakt tussen de opgelegde druk en de gezonde druk om het beveiligingsgedrag uit te oefenen. Imitatie, identificatie en psychologisch matchen zijn de steekwoorden die de indirecte ervaring toebehoren (Malhotra en Galetta, 1999). Het kent echter een overlap met de verbale overtuiging en sociale steun. Computerbeheer is de term die staat voor de hoeveelheid aan computers per huishouden en het soort internetaansluiting. Dit is van belang, omdat een open, draadloos netwerk een optimale beveiliging van de PC noodzaakt, omdat anderen anders in de computer kunnen. Als iemand alleen een internetaansluiting gebruikt zonder netwerk is men uiteraard niet vatbaar voor de gevaren van een netwerk, maar nog steeds wel voor gevaren van het internet.

De mate van controle wordt gemeten door de computerkwantiteit, de onzekerheid en kinderen. De hoeveelheid tijd die wordt doorgebracht achter het internet is van belang vanwege de toename van risicovolle activiteiten. Een persoon die zich voortdurend op het internet begeeft zal een groter risico lopen dat een persoon die af en toe alleen zijn/haar mail bekijkt. De items betreffende kinderen komen vervolgens aan bod als onderdeel van het controleconstruct. De items gaan in op het computergedrag van de kinderen en de mogelijkheid tot besmetting als gevolg van hun gedrag. De onzekerheid komt aanbod bij de items 27^{a} tot en met 27^{e}. Sommige onzekerheidsitems zijn specifieke en concrete items, zoals 27d (" als er een onzekere site is die ik toch wil bekijken, doe ik dat op de UT"). Ook zijn er zeer algemene en abstracte items, zoals 27a ("ik weet precies hoe het internet werkt"). De basis betreft echter de (on)zekerheid die mogelijk ontstaat door de complexiteit van een computer en van het internet en de consequenties ervan. Als bijvoorbeeld de veiligheid van

een Personal Computer in eigen handen ligt (item 27e), heeft dit implicaties voor het gevoel van zekerheid. Men kan zich zekerder gaan voelen, omdat de beveiliging van de PC aan te leren is. Als het item ontkennend wordt ingevuld kan men zich erg onzeker voelen, omdat er geen controle is over de beveiliging van de PC.

2.2.2 Cognitieve respons

De items die de computerangst moeten meten (items 26a tot en met 26f) zijn gebaseerd op de Computer Anxiety Rating Scale (CARS: Heinssen, Glass en Knight, 1987). Uit de literatuur blijkt, dat de voornaamste kenmerken van computerangst betrekking hebben op vermijding, extreme voorzichtigheid, bagatellisering, de verschrikking van virussen en een besmette computer. De CARS vragenlijst is hierop aangepast, zoals uit vraag 26d blijkt: "Ik mijd computers wel eens, omdat ik bang ben dat iemand anders er informatie vanaf kan halen". In de vragenlijst wordt er onderscheid gemaakt tussen computerangst geoperationaliseerd als angst voor de computer als technologie en de angst voor verkeerd (computer)gebruik, waardoor mogelijk de computer besmet kan worden.

De items van de Computer en Internet Self-Efficacy (items 23a tot en met 23f) zijn gebaseerd op de Computer User Self Efficacy scale (CUSE: Cassidy en Eachus, 2002). De Internet Self-efficacy Scale (Torkzadeh en van Dyke, 2001) is een andere belangrijke vragenlijst die door middel van een zelfbeoordeling een zekerheidsgevoel voor een bepaalde internettaak de CISE meet. Deze items zijn niet gebruikt in deze vragenlijst met de reden, dat de zelfeffectiviteit in computerbeveiligingsgedrag niet alleen bestaat uit een gevoel van zekerheid, maar ook uit een bepaalde overtuiging van het eigen kunnen in het geheel. Zekerheid wordt hier als onderdeel van de eigen overtuiging gezien. De CUSE kent een zespunts Likertschaal waarin de respondent zijn/haar mening dient te geven over de stellingen. De items betreffen een algemene toepassing op computers, maar ook enkele eerder genoemde beveiligingstaken. Dit betekent dat sommige items van de CUSE zijn aangepast om de overtuiging betreffende de computerbeveiliging te meten.

De operationalisering van de ervaring betreft de opgedane bekwaamheid. Hierbij kan er gevraagd worden naar de vaardigheden en kennis, maar ook naar het aantal keer dat de ervaring is opgetreden, het leerproces voor de bekwaamheid. Durndell en Haag (2002) hebben ervaring altijd op een kwantitatieve manier gemeten, bijvoorbeeld de hoeveelheid tijd die is besteed aan een bepaalde taak. Er zijn ook onderzoekers die de ervaring kwalitatief meten. Het kost in dit geval te veel tijd om van alle respondenten te observeren hoe goed ze een antivirus kunnen opzoeken en installeren. De competentie van de respondent wordt gemeten door het geven van een algemeen rapportcijfer voor computerdeskundigheid (item 20) en in cijfers voor de deelhandelingen (item 24).Om de ervaring met de betreffende gedragsregels te meten wordt er van de respondent gevraagd om een inschatting te maken over de kwantiteit aan ervaring betreffende de eerder genoemde preventiemaatregelen (item 22a tot en met d).

De uitkomstverwachtingen komen hier aan bod (items 21 a tot en met 21f). Bij de operationalisatie van de uitkomstverwachtingen komt met name het verwachte voordeel van het risicogedrag aan bod, wat ten koste gaat van het nadeel van het risicogedrag. De verwachte consequenties worden opgedeeld in fysieke, sociale en zelfevaluatieve uitkomsten en de risico's ten opzichte van de voordelen. Er worden een aantal handelingen aangehaald waarbij er een risicogedrag kan ontstaan doordat er bepaalde voordelen zijn die prioriteit

krijgen boven correct beveiligingsgedrag. Uit de literatuur van Alhakami en Slovic (1994) blijkt, dat als er veel positieve uitkomsten worden verwacht, er minder aan de risico's wordt gedacht. Het gevolg hiervan is, dat er meer risico's worden genomen. Het downloaden van muziek of gemakkelijke wachtwoorden zijn hiervan voorbeelden. Chatten heeft veel sociale uitkomsten die erg voordelig kunnen zijn. Zelfevaluatie wordt gerealiseerd door beantwoording van de stellingen.

2.2.3 Affectieve respons

De attitudemeting is gebaseerd op de Computer Attitude Scale (CAS: Nickel en Pinto, 1986). Er is ook gekeken naar de Internet Attitude Items (Durndell en Haag, 2002), die op de CAS is gebaseerd. In de literatuur wordt attitude beschreven als een positieve of negatieve reactie op computerbeveiliging en als reactie op beveiligingsmechanismen (Torkzadeh en van Dyke, 2002). In Stephens en Creaser (2001) wordt de computerattitude omschreven in termen als interesse, vermaak en gevoelens.

De items betreffende vertrouwen komen vervolgens aan bod (items 19a tot en met 19g). Op basis van de theorie van Corritore e.a. (2003, 2005) kan gesteld worden, dat de geloofwaardigheid van het internet en de preventieregels belangrijk zijn bij de operationalisatie van vertrouwen. De geloofwaardigheid is verdeeld in eerlijkheid, expertise, voorspelbaarheid en reputatie van de regels tegen virusbesmetting, waarnaar de items geconstrueerd zijn.

2.2.4 Gedragsrespons

De stellingen die het computerbeveiligingsgedrag beogen te meten komen aan bod in de items 17b tot en met 17h van de vragenlijst (bijlage III). Zoals in paragraaf 1.1 te lezen is, zijn er een aantal gedragsregels die een bijdrage kunnen leveren aan een onbesmette computer. De items die de gedragsrespons meten zijn een operationalisering van deze regels. De respondent moet aangegeven in hoeverre het eindgedrag, namelijk de uitvoering van de regels voor een betere computerbeveiliging, wordt uitgeoefend.

2.3 Pilot

Voordat de vragenlijst wordt afgenomen bij de doelgroep, hebben een aantal deskundige mensen de vragenlijst eerst getest. Het doel van deze pilot is het verkrijgen van feedback over de af te nemen vragenlijst. Ongeveer tien mensen hebben de vragenlijst ingevuld en er was sprake van een consensus in de kritiek. Enkele items werden genoemd, omdat er sprake was van een dubbele vraagstelling. In de definitieve versie van de vragenlijst zijn deze problemen verholpen door een overbodig deel van de vraag weg te laten of door de vraag te veralgemeniseren. Ook bij de vragen 10 en 13 werden veel moeilijkheden geconstateerd door de verplichte toekenning van de cijfers 1 tot en met 10 voor de verschillende antwoorden. Met name de mensen die meerdere internetfuncties nooit gebruiken kunnen de vraag niet correct beantwoorden, omdat het laagste cijfer (1) eenmaal gebruikt mocht worden. Dit probleem is verholpen door de vraagstelling aan te passen. De proefpersoon dient niet meer alle internetfuncties te rangschikken, de eerste vijf volstaan. Ook is er een technisch probleem geweest wat betreft de zogenoemde "skipfunctie". Deze functie zou er bij vraag 11 (hoeveel

kinderen heeft u") voor moeten zorgen dat in het geval van een ontkennend antwoord automatisch wordt doorgeschakeld naar vraag 15. Deze skipfunctie functioneert echter niet naar behoren. Het probleem is ondervangen door achter het ontkennende antwoord tekstueel verwijzen naar de volgende vraag voor respondenten zonder kinderen. Hierdoor zullen er zo min mogelijk respondenten de vragenlijst beëindigen.

2.4 Deelname

De doelgroep wordt gevormd door de studenten en medewerkers van de faculteit Gedragwetenschappen van de Universiteit Twente. De vragenlijst is door middel van het programma "surveymonkey" digitaal afgenomen in de maanden januari en februari 2007. De vragenlijst heeft een periode van drie weken opengestaan. De medewerkers hebben per mail een link ontvangen en zijn uitgenodigd om de vragenlijst via de link in te vullen. De studenten zijn aanvankelijk benaderd via het proefpersonensysteem, wat geen respons opleverde in de eerste vier dagen na plaatsing. Hierna is naar 1065 studenten een mail verstuurd met daarin een uitnodiging om de vragenlijst via de meegestuurde link in te vullen. Hierin is ook vermeld dat de vragenlijst via het proefpersonensysteem te bereiken is.

Als eerste is de vragenlijst ingevuld door veelal medewerkers en vervolgens door de studenten. De vragenlijst is ingevuld door 184 medewerkers en studenten. De groep is onderverdeeld in 109 studenten (59,2%) en 75 medewerkers (40,8%). Tabel 2.1 geeft de demografische samenstelling van de respondentengroep weer. Zoals te zien is, zijn er 111 vrouwen (60,3%) en 73 mannen (39,7%). De gemiddelde leeftijd van de totale groep is 29,6 jaar. Vrouwen zijn gemiddeld 28 jaar en mannen 32 jaar. Van de 111 vrouwen zijn er 69 studentes (62,6%) en 42 medewerkster (37,8%). Van de mannen zijn er 40 student (54,8%) en 33 medewerker (45,2%). De 109 studenten zijn gemiddeld 23,6 jaar en de medewerkers 37,6 jaar oud (zie bijlage IV). Er zijn respondenten die begonnen zijn aan de vragenlijst, maar al zeer snel zijn uitgevallen. De demografische gegevens van de uitvallers zijn niet opvallend, het gaat om 14 medewerkers (7 mannelijk, 7 vrouwelijk) en 16 studenten (7 mannelijk, 9 vrouwelijk). Deze respondenten zijn uit de dataset verwijderd.

Tabel 2.1
Demografische gegevens respondentengroep

	Geslacht	
	Man	Vrouw
Medewerker	33 (18%)	42 (23%)
Student	40 (22%)	69 (37%)
18 t/m 25 jaar	33 (18%)	61 (33%)
25-35 jaar	19 (10%)	29 (16%)
35-45 jaar	6 (3%)	13 (7%)
45-55 jaar	8 (4%)	7 (4%)
55-65 jaar	7 (4%)	1 (1%)

	Man	Vrouw	Student	Mede-werker
1. LBO	1	0	0	1
3. MBO	0	2	0	2
5. HAVO	1	3	1	3
6. HBO	5	13	14	4
7. HBO+	2	3	3	2
8. VWO	14	28	41	1
9. WO	33	51	50	34
10. WO+	17	11	0	28

2.5 Analyse van de interne consistentie

Nadat de data naar een SPSS-file zijn geëxporteerd wordt er eerst gekeken naar de interne consistentie. Om te berekenen of de items meten wat ze beogen te meten wordt de interitem betrouwbaarheid berekend door de Cronbach's alpha voor meetinstrumenten die drie of meer antwoordmogelijkheden hebben (Dooley, 2001, Moore en McCabe, 2002). Door het statistische programma SPSS kan deze alpha worden berekend. Een alpha tussen .60 en .80 is redelijk goed, een alpha tussen .80 en .90 is goed en een alpha van meer dan .90 is uitstekend. Uit de resultaten blijkt, dat de alpha voor elk construct redelijk goed is, behalve voor de constructen die het vertrouwen en de ervaring meten. Tabel 2.2 laat zien, dat met name de angst en volharding, de computerangst en de CISE blijken bij te dragen aan een goed meetinstrument.

Tabel 2.2
Cronbach Alpha, gemiddelde, N en de betreffende items voor de constructen.

	Alpha coëfficiënt	Gemiddelde	N	Betreffende items
Externe stimuli				
Angst en volharding	.76	1,26	166	28 a t/m f
Omgevingsconstruct	.66	2,08	168	15, 17a, 25
Mate van Controle	.83	2.54	26 [1]	9, 14a t/m 14d, 27a t/m d
Cognitieve respons				
Computerangst	.70	1,14	168	26a t/m e
CISE	.81	2,07	171	23a t/m 23f
Ervaring		0,91	174	20, 24, 22a t/m d
Uitkomstverwachtingen	.60	2.78	167	21a t/m 21 f
Affectieve respons				
Attitude	.68	1.96	167	18a, 18b, 18c en 21f
Vertrouwen	.59	1.83	174	19a , 19c t/m 19g
Onzekerheid	.66	2.18	167	18f, 19c, 19c, 27a t/m 27d
Gedrag	*.64*	*3,26*	*168*	*17b t/m 17h*

[1] Alleen respondenten met kinderen kunnen vraag 14 beantwoorden

2.5.1 Externe stimuli

Zoals in tabel 2.2 en 2.3 is te zien, is de betrouwbaarheid van angst en volharding goed. Dat wil zeggen, dat de items die "angst en volharding" meten bijdragen aan een goed meetinstrument. Het construct kent negatieve items, waardoor een positief significant antwoord duidt op een lage mate van angst en volharding. Uit tabel 2.3 wordt duidelijk, dat de items laden op twee factoren. Uit de literatuur blijkt, dat de items die op de eerste factor laden de items betreffen die ingaan op angst. De items die ingaan op volharding laden op de tweede factor. De vraag wordt echter niet verdeeld in twee factoren, omdat beide factoren op een betrouwbare wijze de angst en volharding meten die in dit onderzoek van belang zijn, te weten angst, neuroticisme, angst, hulpeloosheid, stabiliteit, discipline en volharding.

Tabel 2.3
Factoren angst en volharding

Construct angst en volharding (α=. 76)	Angst	Volharding
Ik voel me vaak gespannen en zenuwachtig.	**.89**	.14
Ik maak me vaak zorgen over dingen die mis zouden kunnen gaan.	**.89**	.03
Ik voel me vaak hulpeloos en wil dan graag dat iemand mijn problemen oplost.	**.70**	.39
Ik heb mezelf tamelijk goed in de hand.	.37	**.61**
Ik heb veel zelfdiscipline.	-.05	**.87**
Wanneer een project te moeilijk wordt, ben ik geneigd met iets anders te beginnen.	.21	**.74**

De betrouwbaarheid van de ordinale items van het omgevingsconstruct is ook redelijk goed (α = .66), waardoor het construct bruikbaar is voor verdere analyse. Na factoranalyse blijkt, dat er sprake is van twee factoren. Deze factoren bepalen samen minder dan de helft van de variatie en de afzonderlijke factoren hebben een te lage interne consistentie. Een mogelijke oorzaak voor de verdeling kan liggen in de verschillende omgevingsvariabelen waaruit het omgevingsconstruct bestaat. In de literatuur wordt onderscheid gemaakt tussen de volgende omgevingsvariabelen: sociale steun, verbale persuasie, indirecte ervaring en kwantiteit. Op basis van deze omgevingsvariabelen zijn de items geconstrueerd, dus het kan mogelijk zijn dat de items hierdoor op meerdere factoren laden. De betrouwbaarheid is echter redelijk goed, dus er is geen reden om iets aan het omgevingsconstruct te veranderen. De ratiovariabelen van het omgevingsconstruct (vragen 5, 6, 7 en 8 van de vragenlijst) zijn bedoelt om het computerbeheer te operationaliseren. Factoranalyse wijst uit, dat ratiogeschaalde items en de ordinaal geschaalde items twee verschillende zaken meten. In hoofdstuk 3 komen de resultaten van het omgevingsconstruct aan bod en zullen de frequenties van het computerbeheer besproken worden.

De items die de mate van controle moeten toetsen hebben ook een voldoende interne consistentie (α = .73), maar evenals voorgaande items kent dit construct twee factoren. Hierbij worden twee items weggelaten (items 27_4 en 27_5) vanwege de afwijkende factorladingen. De betrouwbaarheid van het construct verandert hierbij niet. In tabel 2.4 staat een weergave van de factorverdeling. Na de factoranalyse blijkt, dat de twee factoren de mate van controle en de onzekerheid weerspiegelen.
Na verdere betrouwbaarheids- en factoranalyse blijkt, dat de factor onzekerheid uitstekend samengaat met enkele attitude-items (zie tabel 2.5). Voor de betrouwbaarheid van alle constructen zou het een verbetering zijn om de onzekerheid bij de affectieve responsies te plaatsen. De mate van controle zonder de onzekerheidsitems heeft een goede betrouwbaarheid (α = .83) en laadt op een enkele factor.

Tabel 2.4
Construct mate van controle

Construct mate van controle (α=. 73)	Controle	Onzekerheid
Hoeveel uren brengt u thuis op het internet door?	**.34**	.30
Hoeveel toezicht heeft u op het downloadgedrag van uw kinderen?	**.72**	-.10
In hoeverre heeft u afspraken gemaakt met uw kinderen over het downloaden van programma's?	**.93**	-.01
In hoeverre heeft u afspraken gemaakt met uw kinderen over het downloaden van bestanden?	**.96**	-.02
In hoeverre bent u angstig dat uw Personal Computer door toedoen van uw kinderen wordt besmet met een virus?	**.75**	.30
Ik weet precies hoe het internet werkt.	-.12	**.67**
Ik denk dat ik een computer nooit volledig zal begrijpen.	.07	**.91**
Ik denk dat ik computervirussen nooit volledig onder de knie krijg.	.14	**.89**

2.5.2 Cognitieve respons

Tabel 2.2 laat zien, dat de interne consistentie van de constructen die vallen onder de cognitieve respons (computerangst, CISE, ervaring en uitkomstverwachtingen), goed zijn en de constructen als betrouwbaar aangemerkt kunnen worden. De items die computerangst en de CISE representeren hebben naast een goede betrouwbaarheid ook een goede inter-itemcorrelatie. De resultaten van de items die de constructen meten zijn dusdanig goed, dat de items na verwijdering van het item 26f bijdragen aan een betrouwbaar meetinstrument.

Om een indicatie te krijgen van de samenhang met de overige constructen zijn de antwoorden op het ervaringsconstruct op een andere manier verwerkt. Een negatief antwoord heeft een score van 0 gekregen en een positief antwoord heeft een score van 1 gekregen. De verhouding tussen beide ligt op een schaal tussen 0 en 1, net als een correlatiecoëfficiënt. De items die ervaring zouden moeten meten hebben namelijk een slechte betrouwbaarheid. De oorzaak lijkt te liggen in de het meetinstrument. Een adequate inschatting van de eigen ervaring is zeer subjectief, waardoor de antwoorden scheef worden verdeeld. Zoals Beckers en Schmidt (2001) al opmerken in hun onderzoek: het betreft een perceptie die men heeft over de eigen relevante kennis en vaardigheden. Als de respondenten niet op de hoogte zijn van de gestelde beweringen (bijvoorbeeld "mijn computer is besmet geraakt door onbetrouwbare sites als Kazaa, MSN of Limewire) kan er geen correct antwoord gegeven worden. Het is belangrijk dat de resultaten van dit construct als indicatie worden gezien.

De items die de uitkomstverwachtingen meten hebben na verplaatsing van een item een redelijk goede betrouwbaarheid. De items laden echter ook op twee factoren. De oorzaak hiervan zou kunnen liggen in de taakgerichte uitkomsten en de persoonsgerichte uitkomsten, zoals ze in de literatuur ook wel worden gesplitst (Compeau en Higgins, 1995, zie paragraaf 1.2). De ene factor appelleert aan veel persoonlijk voordeel van de risicovolle situatie en de andere appelleert aan veel taakgerichter voordeel van een activiteit. De alphacoëfficiënt van de tweede factor is voldoende (α = .63), maar van de eerste niet (α = .56). Vanwege het verlies aan betrouwbaarheid bij weglating van een item en bij de splitsing in afzonderlijke factoren, wordt er niets aan de samenstelling van het construct veranderd.

2.5.3 Affectieve respons

Zoals eerder is vermeld is er aan de affectieve respons een nieuw construct toegevoegd, namelijk onzekerheid. Sommige onzekerheids- en attitude-items lijken te laden op dezelfde factor. In tabel 2.5 wordt vermeld hoe de items zich verhouden ten opzichte van de factoren. Het resultaat is een nieuw betrouwbaar construct, namelijk de onzekerheid. De items die de attitude meten hebben voldoende interne consistentie. Een opmerking moet worden geplaatst over de meetschaal bij de attitude- en onzekerheidsmeting: een hoge score duidt op een negatieve attitude c.q. weinig onzekerheid.

Tabel 2.5
Items van "attitude" en "onzekerheid"

Items van attitude en de toegevoegde items van onzekerheid	Factor 1: Attitude (α=. 68)	Factor 2: Onzekerheid (α= .66)
Het internet met al zijn risico's geeft me een oncomfortabel gevoel	**.79**	.29
De mogelijke internetrisico's benauwen mij.	**.86**	.15
De mogelijke internetrisico's frustreren mij.	**.63**	.22
Het internet is verantwoordelijk voor veel slechte dingen.	**.58**	-.45
De complexiteit van de methoden om mijn computer te beveiligen schrikt mij af.	.25	**.26**
Ik maak me druk om de beveiliging van mijn computer	.38	**.62**
Ik weet precies hoe het internet werkt.	.25	**.40**
Ik denk dat ik een computer nooit volledig zal begrijpen.	-.02	**.80**
Ik denk dat ik computervirussen nooit helemaal onder de knie krijg.	.15	**.79**

Het construct "Vertrouwen" heeft, na de itemuitwisseling (zie tabel 2.6), een alpha van α= .59. Naar mijn mening is vertrouwen een te omvangrijk concept om in een aantal items te kunnen omvatten. Voor een betere betrouwbaarheid en weinig differentiatie tussen items moet het onderwerp veel omvangrijker bestudeerd worden. De samenhang met de overige constructen staan vermeld in hoofdstuk 3.1.

Tabel 2.6
Betrouwbaarheid, gemiddelde N en de betreffende items van de affectieve constructen

Affectieve respons	Alpha coëfficiënt	Gemiddelde	N	Betreffende items
Attitude	.68	3,47	167	18a, 18b, 18c en 21f
Vertrouwen	.59	1.66	174	19a , 19d t/m 19g
Onzekerheid	.66	2,00	167	19b, 19c, 18f, 27a t/m d

2.5.4 Gedragsrespons

Als laatste komt de gedragsrespons aan bod, die wordt gemeten door een enkel construct, namelijk het eindgedrag: computerbeveiligingsgedrag. Na verwijdering van een item is de betrouwbaarheid redelijk goed (α=.64). De items laden allen op één factor, namelijk het eindgedrag. Het construct draagt bij aan een goed meetinstrument.

Een aantal items die het computerbeheer meten voor het omgevingsconstruct, zijn nog niet gebruikt in de hypothesetoetsing. De reden hiervoor is, dat ze de betrouwbaarheid van het omgevingsconstruct verlagen. Het gaat hier om vraag 5 tot en met 8 (zie vragenlijst in bijlage III), die worden gemeten voor het omgevingsconstruct. Omdat het items zijn met verschillende meetniveaus's kan de onderlinge betrouwbaarheid niet worden gemeten. Er kan echter wel een Pearson correlatiecoëfficiënt worden berekend, wat in paragraaf 3.1 aan bod zal komen.

Resumerend kan gezegd worden, dat de vragenlijst zoals deze is afgenomen een betrouwbaar meetinstrument is gebleken en dat de respons groter is dan verwacht. In het volgende hoofdstuk zal de hypothesetoetsing aan bod komen. Dit gebeurt een de hand van correlaties. De uitkomsten van een correlatieanalyse levert uitspraken over de samenhang tussen twee constructen op. Er zijn geen afhankelijke (te verklaren) en onafhankelijke (verklarende) variabelen. De correlatie wordt vastgesteld door de correlatiecoëfficiënt van Spearman voor minimaal ordinale variabelen en Pearson voor interval- en ratiovariabelen. Het voordeel van correlatie is de eenvoudige weergave van de relatie tussen twee constructen. Ook is de richting van het verband belangrijk voor de conclusies. Het nadeel van correlatie is wel, dat deze sterk bepaald wordt door uitschieters en dat het geen causatie aangeeft (Moore en McCabe, 2002). De resultaten van de dataverwerking komen in hoofdstuk 3 aan bod. De conclusies die worden getrokken op basis van de resultaten worden in hoofdstuk 4 besproken.

Hoofdstuk 3 Resultaten

In paragraaf 1.4 wordt duidelijk dat de aannames die worden gedaan gebaseerd zijn op onderlinge samenhang tussen de constructen uit het onderzoeksmodel. Na analyses over de betrouwbaarheid en de factoren, zijn de correlaties berekend tussen de verschillende constructen (zie correlatietabel in tabel 3.1). In figuur 3.1 aan het einde van dit hoofdstuk worden ten behoeve van het overzicht de correlaties in het onderzoeksmodel geplaatst.

Een algemene blik op de resultaten van het onderzoek (zie tabel 3.1) laat zien, dat het eindgedrag direct samenhangt met angst en volharding, de omgeving, CISE, uitkomstverwachtingen, attitude, onzekerheid en vertrouwen. Ook valt op, dat de affectieve constructen direct samenhangen met het eindgedrag, zoals verondersteld is in hoofdstuk 1. De discussie waar in hoofdstuk 1 over te lezen is komt hier duidelijk naar voren. Tussen CISE, computerangst, attitude en onzekerheid zijn soms sterkte correlaties waar te nemen.

Een blik over de gemiddelden van alle items (zie bijlage IV) laat zien dat veel respondenten aangeven geen kinderen te hebben (gemiddelde V11 = 0,30). Ook geeft men aan gemiddeld ongeveer eens per jaar zich op een computerdeskundige te beroepen (gemiddelde V15 = 1,02). Als het gaat om ervaring, dan geven de respondenten zichzelf een 6,75 gemiddeld (mannen 7,49, vrouwen 6,27). Als het gaat om de rapportcijfers, dan geven de respondenten zichzelf het hoogste cijfer voor het beoordelen van een e-mail (7,73) en het laagste cijfer voor het maken van backups (5,56). Een erg laag gemiddelde is er voor de stelling "ik heb Kazaa op de computer, omdat iedereen dat heeft"(gemiddelde = 0,39). De items over computervermijding (item 26d) en computerangst (items 26e) hebben ook zeer lage gemiddelden, respectievelijk 0,80 en 0,76.

3.1 Hypothesetoetsing

Tabel 3.1
Correlatietabel constructen (N=184) *p<0,05, **p<0,01

	2	3	4	5	6	7	8	9	10	11
1. Angst en volharding	.06	.19	.19*	-.15	.15	.20*	.17**	.18*	.17*	-.21**
2. Omgeving		.08	.30**	-.10	.01	.16*	.21**	.08	.28**	.19*
3. Mate van Controle[1]			.07	-.23	.13	.09	-.27	.03	.39*	.04
4. Computer angst				-.30**	.10	-.06	.52**	.29**	.12	.08
5. CISE					-.19*	.03	-.26**	-.71**	-.07	.23**
6. Ervaring[2]						.14	.02	.11	.11	-.24**
7. Uitkomst verwachtingen							-.23**	.09	.21**	-.39**
8. Attitude								.27**	.02	.26**
9. Onzekerheid									.16*	-.20**
10. Vertrouwen										-.17*
11 Eindgedrag										

[1] Mate van Controle wordt alleen gemeten door de antwoorden van de respondenten met kinderen (N=27).
[2] Indicatie van ervaring.

Hypothese 1
H1a: Leeftijd, professionele oriëntatie, angst en volharding en geslacht, vertonen een significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.
H1o: Leeftijd, professionele oriëntatie angst en volharding en geslacht, vertonen geen significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.

Vanwege de ratioschaal van de items die leeftijd, professionele oriëntatie en geslacht meten wordt voor deze variabelen Pearson correlatiecoëfficiënt berekend. Voor de berekening van de samenhang tussen de angst en volharding en de cognitieve constructen wordt Spearman correlatiecoëfficiënt gebruikt. De coëfficiënt van Spearman wordt gebruikt bij een vergelijking tussen twee ordinale constructen. Tabel 3.1 en 3.2 laten zien, is de significante samenhang tussen angst en volharding en computerangst positief. Dit houdt in, dat een angstiger en onvolhardende persoonlijkheid samenhangt met meer computerangst. Dit geldt ook voor het geslacht. Hoe hoger de score voor geslacht (man= "0"en vrouw= "1"), hoe hoger de computerangst, wat impliceert dat vrouwen iets meer computerangst hebben. De correlatie tussen geslacht en CISE is negatief. Dat houdt in, dat hoe hoger de score voor geslacht (hoe vrouwelijker), hoe minder de CISE is. Ook tussen angst en volharding en positieve uitkomstverwachtingen is een positieve relatie. Een angstiger en onvolhardende persoonlijkheid hangt samen met meer positieve uitkomstverwachtingen.

Een ander opvallend resultaat is de significant negatieve samenhang tussen leeftijd en uitkomstverwachtingen. Dit houdt in, dat hoe ouder de respondent is, hoe minder uitkomstverwachtingen hij/zij heeft. In hoofdstuk vier zal naar voren komen dat dit een samenhang vertoont met risicobeperkend gedrag. De correlatie tussen opleiding en computerangst is significant negatief. Een hogere opleiding hangt samen met minder computerangst. Voor ervaring geldt ook een significante negatieve samenhang, maar deze ligt minder voor de hand. Hoe hoger de opleiding, hoe minder ervaring men heeft met beveiligingsgedrag.

Tabel 3.2
Correlaties externe stimuli en cognitieve respons

	Angst en volharding (N=167)	Leeftijd (N=184)	Geslacht (N=184)	Opleiding (N=184)	Omgeving (N=168)	Controle (N=27)
Computerangst	.19*	.09	.17*	-.28**	.30**	.07
CISE	-.15	.04	-.44**	.18*	-.10	-.23
Ervaring	.15	-.10	.08	-.19**	.01	.13
Uitkomst-Verwachtingen	.20*	-.51**	-.01	-.03	.16*	.09

*p<0,05** p<0,01

Hypothese 2
H2a :Het omgevingsconstruct, bestaande uit verbale persuasie, sociale steun, indirecte ervaring en kwantiteit vertoont een significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.
H2o: Het omgevingsconstruct, bestaande uit verbale persuasie, sociale steun, indirecte ervaring en kwantiteit vertoont geen significante samenhang met cognitieve responsies, die bestaan uit computerangst, CISE, ervaring en uitkomstverwachtingen.

Zoals in tabel 3.1 en 3.2 is te zien, is er een positief significante correlatie tussen de omgeving en de computerangst. Dit houdt in, dat meer sociale steun, persuasie, indirecte ervaring en kwantiteit is gerelateerd is aan meer computerangst. De omgeving hangt ook positief samen met de uitkomstverwachtingen. Dit houdt in, dat de variabelen die de omgeving bepalen samenhangen met betere verwachtingen op een positieve uitkomst. Ook is er een positieve samenhang met attitude en vertrouwen. Dat wil zeggen, dat meer sociale steun, persuasie, indirecte ervaring en kwantiteit is gerelateerd aan meer negatieve attitude en meer vertrouwen, wat erg tegenstrijdig is.

Hypothese 3
H3a: De mate van waargenomen controle, bestaande uit kinderen en kwantiteit vertoont een significante samenhang met cognitieve responsies, bestaande uit computerangstangst, CISE, ervaring en uitkomstverwachtingen.
H3o: De mate van waargenomen controle, bestaande uit kinderen en kwantiteit vertoont geen significante samenhang met de cognitieve responsies, bestaande uit computerangstangst, CISE, ervaring en uitkomstverwachtingen.

Tabel 3.1 laat zien dat de mate van controle, zonder het onzekerheidsconstruct, alleen significant samenhangt met het vertrouwen. Meer controle hangt samen met meer vertrouwen Corritore, 2003). Hierbij moet vermeld worden, dat het controleconstruct een zeer lage deelname kent doordat de vragen de respondenten met kinderen betreffen.

Hypothese 4
H4a: Computerangst vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.
H4o: Computerangst vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.

Zoals tabel 3.1 vermeld, heeft computerangst een significante samenhang met onzekerheid (α =.29**) en attitude (α =.52**). Meer computerangst hangt samen met meer onzekerheid en een meer negatieve attitude. De samenhang tussen computerangst en vertrouwen is niet significant. Een verklaring van dit slechte significantieniveau kan de minder goede betrouwbaarheid van het vertrouwensconstruct zijn. Met het eindgedrag is geen directe correlatie. Uit hypothese 9 blijkt, dat er wel een indirecte relatie bestaat met het eindgedrag, namelijk via de onzekerheid.

Hypothese 5
H5a: De Computer en Internet Zelfeffectiviteit (CISE) vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.
H5o: De Computer en Internet Zelfeffectiviteit (CISE) vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.

Tabel 3.1 laat zien, dat de samenhang tussen CISE en attitude en CISE en onzekerheid significant negatief is. Dit betekent, dat meer zelfeffectiviteit samenhangt met minder onzekerheid en een minder negatieve attitude. Ook is er een directe samenhang met het eindgedrag. Meer zelfeffectiviteit hangt samen met beter computerbeveiligingsgedrag. Zoals hierboven beschreven staat is er ook een directe significante negatieve samenhang met computerangst. Dit houdt in, dat meer zelfeffectiviteit samenhangt met minder computerangst. Ook is er een samenhang met de idicator van ervaring.

Hypothese 6
H6a: Ervaring, bestaande uit competentie en ervaring, vertoont een significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.
H6o: Ervaring, bestaande uit competentie en ervaring, vertoont geen significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.

De ervaring is gemeten door de som van de positieve antwoorden en de som van de negatieve antwoorden. De vergelijking van deze alternatieve coëfficiënt met de andere constructen laat zien, dat er alleen een significante negatieve samenhang is met het eindgedrag en de CISE. Dit houdt in, dat meer ervaring met computerbeveiligingsgedrag samenhangt met minder computerbeveiligingsgedrag. De correlatie met CISE is negatief, wat tegenstrijdig is. Meer zelfeffectiviteit hangt samen met minder ervaring.

Hypothese 7
H7a: Positieve uitkomstverwachtingen vertonen een significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.
H7o: Positieve uitkomstverwachtingen vertonen geen significante samenhang met de affectieve responsies, bestaande uit attitude, onzekerheid en vertrouwen en de gedragsrespons.

De samenhang met attitude is negatief, wat betekent dat een positieve uitkomstverwachting samenhangt met een minder negatieve attitude. Met vertrouwen is een positieve relatie. Een positievere verwachting over de uitkomsten hangt samen met meer vertrouwen. Tussen de uitkomstverwachtingen en het eindgedrag bestaat ook een significante negatieve correlatie bestaat. Zoals in hoofdstuk 1 wordt uitgelegd brengt een positieve verwachting van de uitkomsten, minder computerbeveiligingsgedrag met zich mee. Hoe beter de verwachting van het resultaat, des te minder beveiliging (zie paragraaf 1.2 en 1.3).

Hypothese 8
H8a: Attitude vertoont een significante samenhang met computerbeveiligingsgedrag.
H8o: Attitude vertoont geen significante samenhang met computerbeveiligingsgedrag.

De samenhang tussen attitude en het eindgedrag is significant positief, wat betekent dat H8o verworpen kan worden. Een negatievere attitude hangt samen met meer beveiligingsgedrag. Voorts kent attitude meer significante relaties, zoals uit tabel 3.1 blijkt. Er is een positieve samenhang met angst en volharding, omgeving, computerangst, onzekerheid en het eindgedrag. Er is een negatief significante samenhang met CISE en de uitkomstverwachtingen.

Hypothese 9
H9a: Vertrouwen vertoont een significante samenhang met computerbeveiligingsgedrag.
H9o: Vertrouwen vertoon geen significante samenhang met computerbeveiligingsgedrag.

Vertrouwen vertoont een negatieve significante samenhang met het eindgedrag, hoewel deze niet erg sterk is. Het houdt in, dat meer vertrouwen samenhangt met minder beveiligingsgedrag. De correlatietabel 3.1 laat verder zien, dat vertrouwen een positief significante relatie heeft met de omgevingsfactoren en de uitkomstverwachtingen. Dit houdt in, dat meer sociale steun, verbale overtuiging, indirecte ervaring en een positieve verwachting van de uitkomsten samenhangt met meer vertrouwen.

Hypothese 10
H10a: Onzekerheid vertoont een significante samenhang met computerbeveiligingsgedrag.
H10o: Onzekerheid vertoont geen significante samenhang met computerbeveiligingsgedrag.

Uit de resultaten blijkt, dat onzekerheid een construct is dat niet correleert met de mate van controle. Uit voorgaande beschrijvingen blijkt, dat het de betrouwbaarheid ten goede komt als de onzekerheid als een affectieve respons wordt gezien. Doordat de affectieve stimuli hierdoor niet twee maar drie constructen kent impliceert, dat er een nieuwe hypothese is ontstaan. Tabel 3.1 laat zien dat onzekerheid significant negatief samenhangt met het eindgedrag. Dit houdt in, dat meer onzekerheid samengaat met minder beveiligingsgedrag en dat de H10o verworpen kan worden. Onzekerheid heeft ook een positieve samenhang met angst en volharding, computerangst en attitude. Meer onzekerheid correleert met meer (computer) angst en volharding en meer negatieve attitude. Er is een sterke negatieve samenhang met CISE (α= -.71), wat inhoud dat meer onzekerheid samenhangt met minder CISE.

Overige resultaten

Niet alleen de affectieve constructen hebben een directe invloed op het eindgedrag. Ook de omgeving en de CISE hebben een positieve samenhang met het eindgedrag, Angst en volharding, ervaring en de uitkomstverwachtingen correleren negatief met het gedrag. De hypotheses zijn correct, maar het onderzoeksmodel kan completer worden geconstrueerd (zie figuur 3.2).

In de literatuur in paragraaf 1.2 is beschreven, dat computerangst vaak ook een direct verband heeft met CISE en met het uiteindelijke gedrag. Hoewel dit gegeven uit de literatuur is overgenomen en niet is verwerkt in een hypothese, kan de correlatietabel (tabel 3.1) toch

eenvoudig uitsluitsel geven over de juistheid van deze aanname. Computerangst heeft een negatieve samenhang met de CISE: hoe meer computerangst, hoe minder zelfeffectiviteit. De computerangst heeft een indirecte samenhang met het eindgedrag, namelijk via de attitude en onzekerheid respons.
Positievere uitkomstverwachtingen hangen samen met een lagere leeftijd (zie tabel 3.2). Dit impliceert dat leeftijd een indirecte invloed heeft op het eindgedrag, namelijk via de uitkomstverwachtingen. Hoe jonger men is, hoe positiever de uitkomstverwachtingen, hoe minder het computerbeveiligingsgedrag.

Uit de items van vraag 10 (zie bijage III voor de vragenlijst) blijkt, dat mensen het internet het meest gebruiken voor de e-mail, voor het zoeken naar informatie en chatten, bijvoorbeeld via MSN. De laatste activiteit kan gevaarlijk zijn, omdat via MSN veel spyware op de computer wordt geïnstalleerd. De activiteiten die mogelijk gevaarlijk zouden kunnen zijn worden het minst uitgevoerd, namelijk creditcardaankopen doen en administratie zoals online bankieren, bealstingaangifte en Didid gebruik.

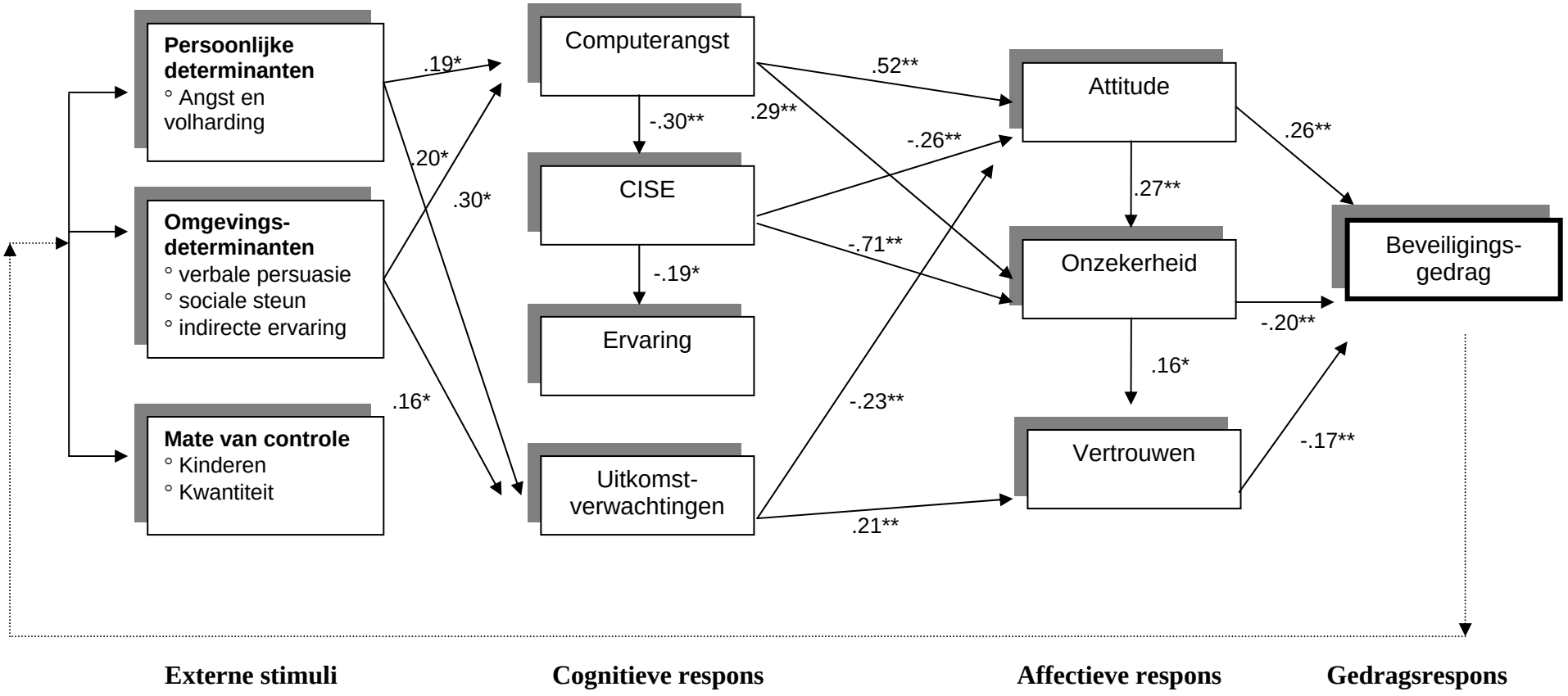
Tabel 3.3
Pearson correlaties computerbeheer (N=184)

	1	2	3	4
1. Hoeveelheid PC's		-.16*	-.21**	.20**
2. Draadloze internetverbinding			.69**	-.46**
3. Draadloos netwerk				-.44**
4. Laptopgebruik				

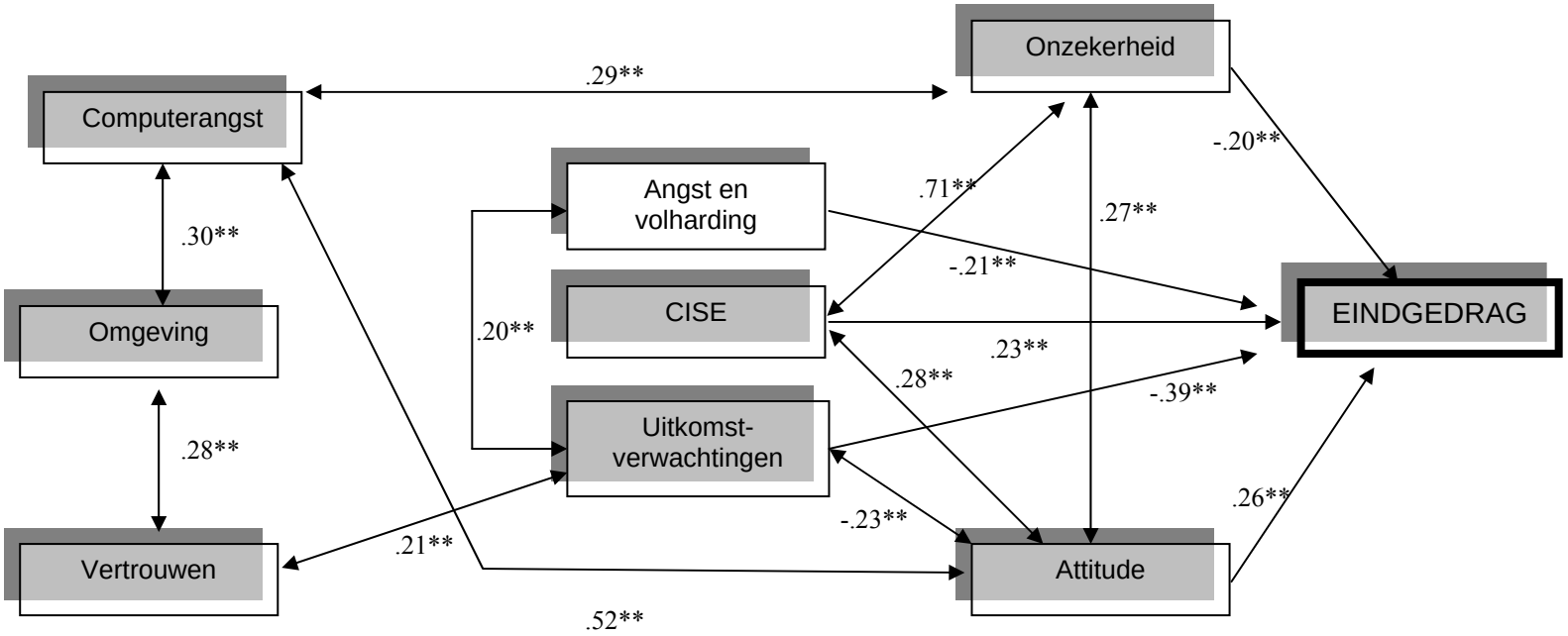
*p<0,05, ** p<0,01

De samenhang tussen de items betreffende computerbeheer staat vermeld in tabel 3.3. Uit deze Pearson correlatiecoëfficiënten blijkt, dat er een negatieve samenhang is tussen de hoeveelheid aan Personal Computers in het huishouden en het gebruik van een draadloze internetverbinding en een draadloos netwerk. Dat houdt in, dat meer computers in huis samenhangt met meer draadloze internetverbinding en meer draadloos thuisnetwerk heeft. De reden hiervoor is de omgekeerde schaling. Ook hangt de hoeveelheid PC's positief samen met laptop gebruik. Hoe meer PC's in huis zijn, hoe meer laptops er gebruikt worden. Het komt erop neer, dat huishoudens met meerdere Personal Computers eerder een draadloos netwerk en een draadloze internetverbinding hebben. Ook hangt het samen met het internetten via de laptop. Hoe meer PC's er in huis zijn, hoe meer er gebruik wordt gemaakt van een laptop om te internetten.

Het gebruik van een draadloze internetverbinding hangt goed samen met een draadloos netwerk (r =.69**). Het laptopgebruik correleert significant negatief met een draadloze internetverbinding en het draadloze netwerk. Dit houdt in, dat mensen die vaker een laptop gebruiken, meer gebruiken maken van draadloos internet.



Figuur 3.1
Significante correlaties hypotheses



Figuur 3.2
Model van significante resultaten ≥ (-).20

Hoofdstuk 4 Discussie

Op basis van de aannames en de resultaten kunnen de gevolgen van de resultaten worden verwoord. In paragraaf 4.1 zal de deelname worden besproken, evenals de conclusies over de interne consistentie en de factoranalyses. De conclusies over de samenhang tussen de constructen komt in paragraaf 4.2 aan bod.

4.1 Respons en kwaliteit

De deelname aan het onderzoek is goed verlopen (N=184). Het voordeel van een onlinevragenlijst is dat veel mensen op een vrij eenvoudige wijze te benaderen zijn en dat de invoer van de data snel en accuraat gebeurt. Een gebleken nadeel van een online-vragenlijst is het gebrek aan overzicht voor de respondent.

De respondenten vertegenwoordigen een homogene groep. Er zijn iets meer studenten dan medewerkers die de vragenlijst hebben ingevuld. Over de leeftijd kan worden gezegd, dat met name die van de medewerkers lager ligt dan de verwachting. De gemiddelde leeftijd van de medewerkers die hebben gereageerd is 38,4 jaar.

Over de kwaliteit van het meetinstrument kan gezegd worden dat deze redelijk betrouwbaar is. Met name de angst en volharding, computerangst, CISE, onzekerheid, attitude en het eindgedrag zijn constructen die een redelijk goede interne consistentie hebben en een goede samenhang tussen de items hebben.

Het construct betreffende angst en volharding heeft een goede interne consistentie en laadt op twee factoren. Dit komt overeen met de literatuur over angst en volharding. Ook komt dit goed overeen met de onderbouwing van de items. De drie items betreffende angst komen uit de angstschaal van de NEO-PI-R en de vragen die volharding meten komen zijn gebaseerd op de volhardingschaal van de NEO-PI-R.

Bij de betrouwbaarheidsmeting van het omgevingsconstruct worden de items betreffende het computerbeheer niet meegenomen vanwege de verschillende meetniveaus. Er is sprake van een lading op twee factoren, die te verklaren is door de variabelen uit het onderzoeksmodel. Enkele items hebben te maken met sociale steun, enkele met sociale persuasie en anderen op de indirecte ervaring.

De items die de mate van controle trachten te meten komen niet geheel met elkaar overeen. Daarom is er gekozen voor een herconstruering van "mate van controle". De alphacoëfficiënt tussen de items van vraag 14 en 9 is voldoende goed (α= .83) en alle items laden op één factor (mate van controle). Het onderzoeksmodel kent dus een verkeerde aanname: de variabele "onzekerheid" vertoont geen samenhang met de mate van controle en alle andere variabelen die de mate van controle voorstellen. Er is wel een significante samenhang met de affectieve respons, waardoor de "onzekerheid" een andere plaats krijgt in het onderzoeksmodel.

De items die de computerangst meten zijn gebaseerd op de Computer Anxiety Rating Scale (CARS: Heinssen, Glass en Knight, 1987). De items zijn gebaseerd op de voornaamste kenmerken van computerangst, namelijk op vermijding, extreme voorzichtigheid,

bagatellisering en de verschrikking van virussen en een besmette computer. Er is een redelijk goede betrouwbaarheid.

De CISE is gebaseerd op de CUSE (Cassidy en Eachus, 2002) en de Internet Self-efficacy Scale (Torkzadeh en van Dyke, 2001). De items die uit de twee vragenlijsten zijn gehaald en de (kleine) aanpassingen ervan zorgen voor een voldoende goede inter-itemcorrelatie.

De items van ervaring zijn weinig betrouwbaar. De oorzaak hiervan kan gelegen zijn in de vraagstelling. Er is onvoldoende rekening gehouden met het feit, dat mensen misschien een gebrekkige zelfreflectie hebben als het gaat om competentie en kennismeting. Als er geen referentiekader is voor mensen is de zelfbeoordeling lastig. Zoals eerder is gemeld, wordt er gewerkt met een indicator.

De items die de uitkomstverwachtingen meten laden op twee factoren. Deze factoren kunnen worden verklaard door de literatuur. Compeau en Higgins (1995) hebben in hun onderzoek de uitkomstverwachtingen verdeeld in taakgerichte uitkomsten en persoonlijke uitkomsten. De items betreffende het risico dat mensen ondergaan om te kunnen chatten en muziek downloaden hebben een meer persoonlijke uitkomstverwachting. De items die de taakgerichte uitkomstverwachtingen meten gaan over bijvoorbeeld het verkrijgen van informatie. Een onderverdeling in deze factoren levert voor de tweede factor een slechte betrouwbaarheid op.

De operationalisatie van attitude is gebaseerd op de Computer Attitude Scale (Nickel en Pinto, 1986) en de Internet Attitude Items (Durndell en Haag, 2002). Deze blijkt betrouwbaar te zijn. De items die het construct vertrouwen trachten te meten kunnen gebruikt worden, maar hebben een betrouwbaarheid die aan de lage kant is. De items die de onzekerheid meten hebben een redelijk goede betrouwbaarheid.

4.2 Conclusies correlatie-analyses

Als naar de opzet van dit onderzoek wordt gekeken kan worden geconcludeerd, dat de factoren die risicoperceptie kenmerken (Ropeik, 2004) niet gemakkelijk in het onderzoeksmodel geplaatst kunnen worden. De veronderstelde relatie tussen mate van controle en vertrouwen is wel bevestigd (Corrtitore e.a., 2003). Ook wordt de bestaande discussie in de literatuur ondersteund door de samenhang tussen CISE, computerangst, attitude en onzekerheid. De TAM kan gedeeltelijk worden bevestigd. Veel constructen hebben een indirect effect op het eindbedrag, waarbij attitude een belangrijke rol speelt. Dit is voorspelt door de TAM. Ook hebben de uitkomstverwachtingen een directe relatie met het eindgedrag. De relatie tussen CISE en het eindgedrag is echter niet conform de TAM. Het model van Compeau en Higgins (1995) wordt ook gedeeltelijk bevestigd. De CSE heeft hier een directe relatie met het eindgedrag en de omgevingsvariabelen hebben een indirect effect via de CSE en de uitkomstverwachtingen. Dit is bevestigd. Het grote verschil met dit model is het beperkte effect van het affect. Ook heeft computerangst een directe relatie met het eindgedrag, wat niet wort bevestigd in het huidige onderzoek. Het model van Marakas e.a. (1998) is erg omvangrijk om helemaal te evalueren. Het belangrijkste is echter, dat CISE hier een grote rol speelt, wat wordt bevestigd goor huidige resultaten. Aan de hand van de bestaande structuur van het onderzoeksmodel (zie figuur 1.7 en 3.1) zal hieronder beschreven

worden wat de verdere implicaties van de resultaten zijn voor de onderbouwing van het onderzoek en de uiteindelijke uitkomsten.

4.2.1 Externe stimuli

Zoals in tabel 3.1 en in tabel 3.2 is te zien, wordt het eindgedrag op twee manieren door de angst en volharding beïnvloed: op een directe manier en op een indirecte manier via de computerangst en uitkomstverwachtingen. Wat in de literatuur te lezen is, is dat de persoonlijke angst of angst als persoonlijkheidskenmerk een indirect effect heeft op het eindgedrag (McFarland en Higgins, 2006; Brosnan, 1998; Igbaria, 1995; Wilfong, 2006). Dit kan worden weerlegd door de huidige resultaten. Er is een indirecte samenhang van het gedrag via de attitude, onzekerheid, vertrouwen en uitkomstverwachtingen, maar ook een directe samenhang van de persoonlijkheid met het computerbeveiligingsgedrag.

De relatie tussen angst en volharing en computerangst (α = .19*) houdt in, dat meer onvolharding en angst, samenhangt met meer computerangst. Computerangst kan worden gezien als een toepassing (een cognitieve respons) van persoonlijke angst en volharding, dus de redelijk lage significante correlatie is onverwacht. Het bevestigd wel, dat er sprake is van twee soorten angst, nameliujk een aangeboren en een toegepaste angst.

In het onderzoeksmodel is de cognitieve respons is een beïnvloeder van de attitude: de specifieke computerangst hangt samen met een negatieve attitude. Met CISE is er een indirecte relatie. Dit is in tegenstelling tot de literatuur van Marakas e.a. (1998) die volharding een directe voorspeller van CISE noemt. Een angstige persoonlijkheid hangt samen met een grotere computerangst en die angst hangt op zijn beurt weer direct samen met de CISE, wat een indirecte samenhang impliceert. Het model van Marakas e.a. (1998) stelt dat volharding direct samenhangt met de CISE, ervaring en de uitkomstverwachtingen. In dit onderzoek kan alleen de laatste significant worden bevestigd, hoewel dit verband niet erg sterk is.

Net als de angst en volharding zijn de attitude-items zijn ook negatief geschaald. Dit houdt in dat een lagere mate van volharding en angst direct samenhangt met een negatievere attitude. De correlaties met onzekerheid en vertrouwen zijn ook positief. Meer angst en volharding leiden tot meer vertrouwen en meer onzekerheid, terwijl in het onderzoeksmodel een indirecte samenhang met alle affectieve responsen wordt gesuggereerd. De positieve relatie met vertrouwen is op het eerste gezicht onverwacht. Het is mogelijk dat vertrouwen een aageboren factor kent. De items die vertrouwen meten zijn echter dusdanig gesteld, dat vertrouwen negatief is. De items zijn gericht op een teveel aan vertrouwen, wat gevaarlijk kan zijn voor het gedrag op het internet.

De leeftijd van de respondent hangt negatief samen met de uitkomstverwachtingen, wat niet terug is te vinden in de aangehaalde literatuur. Er kan gezegd worden, dat hoe ouder mensen worden, hoe minder positief de uitkomstverwachtingen zijn. Dit heeft voor het beveiligingsgedrag positieve consequenties, want hoe negatiever de verwachte uitkomst is, hoe meer mensen zich gaan beschermen (zie paragraaf 1.3).

Een andere externe stimulus is de genoten opleiding. De resultaten wijzen uit, dat opleiding negatief correleert met computerangst, evenals ervaring. Hoe hoger de opleiding is, des te minder de computerangst en ervaring. De literatuur beweert het tegengestelde, namelijk

dat een hoog opleidingsniveau duidt op een hogere CISE door een toename in ervaring. Ervaring is hier een indicatie, dus uitspraken kunnen niet worden gedaan. De correlatie tussen opleiding en CISE kan ook niet worden bevestigd door de resultaten. Feit is wel, dat de respondentengroep homogeen is wat betreft opleidingniveau. Het gaat, net als alle conclusies, om de resultaten van de medewerkers en studenten van de faculteit Gedragswetenschappen op de Universiteit Twente. Als laatste wordt de positieve correlatie tussen geslacht en de CISE genoemd. Torkzadeh en van Dyke (2002) komen in hun onderzoek tot de conclusie, dat mannen een hogere Internet Self-efficacy dan vrouwen. In dit onderzoek kan dezelfde conclusie worden getrokken.

4.2.2 Omgeving

Kijkende naar tabel 3.1 valt op, dat het omgevingsconstruct positief met computerangst correleert. Naarmate mensen meer sociale steun, verbale persuasie en indirecte ervaring ontvangen, hoe meer computerangst er ontstaat. Deze relatie lijkt onlogisch, maar de oorzaak van de significante positieve samenhang met computerangst lijkt te wijten te zijn aan de verbale persuasie en de indirecte ervaring. De items betreffende sociale steun zijn summier, dus de verbale overtuiging en de indirecte ervaring zorgen voor een toename in de computerangst. De sociale druk heeft dus niet alleen invloed op de zelfeffectiviteit (Brosnan, 1998; Marakas e.a., 1998), maar ook op de computerangst.

Ook met de uitkomstverwachtingen bestaat er een positief significante samenhang. Dit houdt in, naarmate mensen meer sociale steun, persuasie en indirecte ervaring krijgen, men meer positieve verwachtingen van de uitkomsten van het gedrag heeft. Hierdoor zal men meer risico nemen en het eindgedrag zal verminderen (zie hypothese 7).

Opmerkelijk is het significant positieve verband met het vertrouwen (r=.30**). Dit houdt in dat meer sociale steun, persuasie en indirecte ervaring samenhangen met meer vertrouwen. Of dit een werkelijk positieve gevolgen heeft met betrekking tot het gedrag met betrekking tot de internetbeveiliging is niet zeker. Het is wel eigenaardig dat mensen meer angst en meer vertrouwen hebben door het omgevingsconstruct. In paragraaf 1.3 is te lezen, dat als mensen vertrouwd zijn de risicoperceptie laag zal zijn. Hierdoor zal men minder zorgen hebben voor de risicowering. Malhotra en Galetta (1999) verklaren, dat wanneer sociale invloed een gevoel van onderworpenheid bewerkstelligt, het een negatieve invloed heeft op attitude en dus op het gebruik van computers. De positieve significante correlatie wijst op een negatieve attitude. Hieruit kan worden opgemaakt, dat de respondenten zich onderworpen hebben gevoeld. Hieruit is op te merken dat de invloed vanuit de omgeving wel als vertrouwd wordt beschouwd, maar negatief is voor het daadwerkelijke beveiligingsgedrag.

De gedragsrespons (het eindgedrag) correleert ook significant positief met het omgevingsconstruct, hoewel niet overtuigend. Dat persoon, omgeving en gedrag met elkaar samenhangen is één van de basisprincipes van Bandura (zie paragraaf 1.2). De resultaten van het correlatieonderzoek tussen het omgevingsconstruct, de angst en volharding en het gedrag onderschrijven dit. Om tot het gedrag te komen zou de effectiviteitverwachtingen volgens het model van Bandura (zie figuur 1.1) ook een rol moeten spelen, maar dat wordt hier niet bewezen. Het resultaat wijkt af van de TAM, die voorspelt dat omgevingsfactoren een indirecte rolspelen op het eindgedrag en attitude en een directe invloed hebben op CISE en

uitkomstverwachtingen. Met de CISE bestaat alleen een indirecte relatie, namelijk via de uitkomstverwachtingen, computerangst en attitude. Dit is tegenstrijdig met de uitkomsten van de studies van Compeau en Higgins (1995) en Brosnan (1998).

Wat een mogelijkheid zou kunnen zijn bij toekomstige bestudering van dit onderwerp is, dat het omgevingsconstruct niet alleen een rol speelt vóór cognitieve verwerking, maar ook daarna, zoals Bandura in zijn theorie al verwoord (zie paragraaf 1.2.1). De factoranalyse wijst uit, dat het construct laadt op twee factoren, hetgeen kan betekenen dat de ene factor goed voor de cognitieve respons geplaatst kan worden en de andere factor goed na de cognitieve respons past. De ene factor kan positiegf zijn (sociale steun) en de andere kan negatief zijn (persuasie). Dit verklaart waarom vertrouwen en attitude correleren met het omgevings-construct en het verklaart waarom omgeving correleert met gedrag. Ook zou de samenhang met angst en uitkomstverwachtingen zou nog kunnen bestaan. Misschien dat er allicht een omgevingsvariabele geconstrueerd kan worden die laadt op een affectieve respons. Dat kan de hoge correlaties verklaren tussen de omgeving, het affect en het gedrag.

4.2.3 Mate van Controle

De samenhang van de constructen van het onderzoeksmodel wordt beschreven in paragraaf 1.3. De literatuur stelt, dat een grote mate van controle over het gedrag minder bedreiging teweegbrengt. De mate van controle vertoont maar één samenhang met de andere constructen uit het onderzoeksmodel en dat is de samenhang met vertrouwen, zoals in de literatuur ook al is gesuggereerd (Corritore, 2003). Meer controle is gerelateerd met meer vertrouwen. De items die uiteindelijk overblijven na afscheiding van de items die de onzekerheid trachten te meten, hebben betrekking op kinderen en de hoeveelheid computertijd. De items die betrekking hebben op kinderen zijn ingevuld door 27 proefpersonen, wat ervoor zorgt dat de resultaten slecht te generaliseren is. Het overige item is wel door voldoende respondenten ingevuld. Naar mijn mening operationaliseren de twee niet voldoende de mate van controle.

Mocht het construct in toekomstig onderzoek toch aan bod komen zou het een aanbeveling zijn het construct nog beter literair te verantwoorden. Ook verdient het de aanbeveling om de plaats in het model te onderzoeken. Mogelijk is er niet alleen bij het onzekerheidsconstruct, maar ook bij het controleconstruct sprake van een affectieve respons. Als mensen geen controle ervaren over een risico, zullen ze er ook minder vertrouwen hebben. Als construct in een onderzoek als deze is er te weinig ruimte om het construct tot zijn recht te laten komen.

4.3.4 Computerangst

Het meest opvallende resultaat is de positief significante relatie tussen computerangst en (negatieve) attitude en onzekerheid, zoals in de literatuur al in gesuggereerd. Een toename van computerangst hangt samen met een toename in negatieve attitude en in onzekerheid. McFarland en Higgins (2006) zien angst als een affectieve staat, wat gezien de resultaten in dit onderzoek aannemelijk is. Ook Lazar e.a. (2006) beschrijven in hun onderzoek de relatie tussen angst en attitude. De relatie tussen computerangst en onzekerheid is in de risicperceptie

een erkende correlatie (Ropeik, 2004). Als men de angst verder wil onderzoeken zal er dus een specifiekere definitie gebruikt moeten worden. De definitie zoals deze in dit onderzoek is gebruikt ziet angst als cognitie en als emotie (Bozionelos, 2001). Dit strookt met de TAM, die de twee responsies strikt laat scheiden. Beckers en Schmidt (2001) zien affect als een onderdeel van de cognitieve beleving van angst. De resultaten kunnen deels de theorie van Beckers en Schmidt (2001) ondersteunen. Het onderzoeksmodel in deze studie probeert een gedrag te verklaren met als onderdeel computerangst, de computerangst is niet de eindvariabele.

Het model van Compeau en Higgins (1995) plaatst angst tussen CSE en het gebruik van computers (eindgedrag). De intermediaire functie van de CISE met de computerangst wordt bevestigd. Er is een significante relatie tussen de CISE en de computerangst. Het gevolg van een toename in computerangst zal een afname van zelfeffectiviteit zijn. De CISE heeft vervolgens een directe positieve samenhang met het eindgedrag (zie hypothese 5), wat de indirecte relatie tussen computerangst en het eindgedrag bevestigt. Hoe groter de overtuiging is van het eigen kunnen in betrekking tot computerbeveiligingsgedrag, hoe groter de kans is dat een goed beveiligingsgedrag wordt uitgevoerd. Hoe lager de computerangst, hoe lager de CISE, dus zal de kans op uitvoering van het eindgedrag lager zijn. Er is echter geen relatie tussen angst en affect is hun model en dat geldt niet voor huidige resultaten.

Wilfong (2006) heeft bewezen, dat computerangst kan ontstaan door gebrek aan ervaring of een slechte ervaring. In deze studie kan dit niet worden bevestigd. Niet alleen wegens het gebrek aan betrouwbaarheid van het ervaringsconstruct, maar ook vanwege de slechte significantie van de correlatie.Voor een volgend onderzoek zou het interessant zijn om deze relatie te bevestigen.

Ook is gebleken dat vrouwen gemiddeld meer computerangst hebben dan mannen, zoals onderzoek al heeft bewezen (Stephens en Creaser, 2001; Durndell en Haag, 2002; Beckers en Schmidt, 2003). In sommige studies wordt het tegendeel beweerd (Brosnan e.a., 1998).

4.2.5 CISE

Compeau en Higgins (1995) spreken van een computer zelfeffectiviteit (CSE) en Torkzadeh en van Dycke (2002) zelfs over internetzelfeffectiviteit. Computer –en internetzelfeffectiviteit (CISE) wordt omschreven als de sterkste overtuiging van de eigen effectiviteit als het gaat om computer -en internettaken. Uit de literatuur blijk, dat mensen met een lage zelfeffectiviteit worden geassocieerd met meer angst en depressie (Luszczynska en Schwarzer in: Connor en Noman, 2005). Mensen met een hoge CSE hebben minder angst, meer voldoening moeten voelen en meer ervaring. De conclusie op basis van de data uit dit onderzoek is, dat de correlaties tussen de constructen overeen komen met deze literatuur. Zoals eerder besproken is er een significant negatieve correlatie met computerangst (Wilfong, 2006). Dit geldt overigens niet voor de angst en volharding. Dit houdt in, dat een lage mate van CISE niet wordt veroorzaakt door angst en volharding als persoonlijkheidseigenschap, maar door de cognitieve verwerking van de angst en volharding.

Zoals in de correlatietabel 3.1 is te aanschouwen, heeft CISE een negatieve significante correlatie met attitude en onzekerheid. Mensen met een sterke overtuiging van de

eigen effectiviteit in computer- en internettaken hebben een minder negatieve attitude en minder onzekerheid. De laatste samenhang heeft een redelijk hoge correlatie, wat aangeeft dat de voorspelbaarheid van de relatie in toekomstig gedrag groot is. Niet alleen heeft CISE een indirect effect op het eindgedrag, maar ook een direct effect. Compeau en Higgins (1995) hebben deze relatie eerder bewezen. Net als in hun model heeft CISE ook in dit onderzoek een significant samenhang met het eindgedrag, met angst en met het affect (Compeau en Higgins, 1995; McFarland en Higgins, 2006). Het model van MArakas e.a. (1998) voorspeld ook een grote mediërende functie voor de CSE. De Tam wordt hier niet bevestigd. De TAM gaat er vanuit dat de waargenomen bruikbaarheid (is gelijkgesteld aan CISE) een indirecte relatie heeft met het eindgedrag.

Ervaring, indirecte ervaring, verbale overtuiging en emotionele factoren worden vaak als bron van SE gezien (zie paragraaf 1.2). In de literatuur komt naar voren, dat kwantiteit een rol speelt bij CISE (Torkzadeh en van Dycke, 2002). Hoe meer ervaring mensen op doen, hoe meer overtuigd ze van zichzelf worden. De ervaring hangt hier echter significant negatief samen met CISE (α=.-19*), wat wil zeggen dat meer zelfeffectiviteit samenhangt met minder ervaring. Dit spreekt alle literatuur tegen. De relatie tussen CISE en ervaring kan in de toekomst een onderzoeksdoel kunnen zijn. Het omgevingsconstruct hangt niet significant samen met CISE. Het bewijs voor de correlatie met indirecte ervaring is ook niet sterk genoeg om er uitspraken over te doen.

Uit de resultaten blijkt, dat vrouwen iets minder op het internet doorbrengen dan mannen. Dit verklaart mogelijk het resultaat, dat mannen hoger scoren op CISE dan vrouwen.

4.2.6 Ervaring

In de literatuur van veel wetenschappers is ervaring een belangrijk construct in de totstandkoming en in standhouding van gedrag. Positieve ervaring hangt samen met een grotere CISE (Beas en Salanova, 2006; Beckers en Schmidt, 2001; Igbaria, 1995). Zoals in paragraaf 1.2 is te lezen is ervaring op te delen in de kennis (directe ervaring) en de bekwaamheid van bepaalde handelingen (competenties). Dit is teruggekoppeld op de beveiligingsbasisregels die in paragraaf 1.1 aan bod zijn gekomen. Het rapportcijfer dat uit vraag 20 blijkt is een goede weergave van de mate bekwaamheid die mensen zichzelf toekennen. Hieruit blijkt, dat mannen zichzelf iets ervarener vinden (gemiddeld 7,49) dan vrouwen (gemiddeld 6,27).Vanwege de tienpuntschaal is dit echter niet te vergelijken met andere constructen. Vraag 22 heeft wel een zespuntschaal, waardoor het op wel vergelijkbaar is. De antwoordverdeling is echter dusdanig scheef, dat de antwoorden niet bruikbaar zijn voor een correlatieberekening. Het resultaat kan alleen als indicator worden gebruikt.
De indicator correleert significant negatief met het eindgedrag, met de CISE en met het opleidingsniveau. Dit wil zeggen, dat meer ervaring samenhangt met minder beveiligingsgedrag, met minder CISE en een minder hoog opleidingsniveau. Dit strookt met de bevinding dat ervaring een positieve invloed heeft op computergedrag (McFarland en Higgins, 2006; Torkzadeh en van Dycke, 2002; Torkzadeh e.a., 2006). Hierbij moet wel gezegd worden, dat computergedrag iets anders blijkt te zijn dan computerbeveiligingsgedrag, omdat de aspecten die computergedrag positief maakt, de risicoperceptie doet verminderen. Dit komt het beveiligingsgedrag niet ten goede (zie hypothese 7).

Zoals in paragraaf 3.1 al is verwoord, het is moeilijk om zelf adequaat te rapporteren welke (negatieve) ervaringen iemand heeft met computerbeveiliging. Uit de literatuur blijkt, dat programma's als Limewire, MSN en Kazaa vrijwel altijd spyware of virussen met zich meebrengen. Ook blijkt uit de literatuur dat deze programma's razend populair zijn en dat veel mensen één van deze programma's op de computer hebben geïnstalleerd. Op de vraag of de computer van de respondent besmet is geraakt door onbetrouwbare sites als Kazaa, Limewire of MSN geeft men gemiddeld een ontkennend antwoord. De oorzaak van de slechte betrouwbaarheid kan worden toegeschreven aan de ondoordachte vraagstelling. Zelfrapportage blijkt wel het juiste middel om ervaring te meten in een soortgelijk onderzoek vanwege de grote efficiency. De subjectiviteit van de zelfmeting van ervaring is een aspect van erving waar goed over nagedacht moet worden.

4.2.7 Uitkomstverwachtingen

De uitkomstverwachtingen worden in paragraaf 1.2 geformuleerd als: "de schatting van een individu dat een bepaald gedrag zal leiden tot bepaalde uitkomsten"(Luszczynska en Schwarzer in: Connor en Norman, 2005). Uit de risicoliteratuur (zie paragraaf 1.3) blijkt, dat als mensen veel voordelen zien, ze minder risico zien, wat ertoe leidt dat mensen gevaarlijker gedrag zullen vertonen (Alhakami en Slovic, 1994). Een positieve verwachting van de uitkomsten zal dus moeten leiden tot minder goed internetbeveiligingsgedrag. De resultaten (zie tabel 3.1) laten zien dat deze aanname correct is, zoals al eerder is bewezen (Compeau en Higgins, 1995). De uitkomstverwachtingen hebben een directe significant negatieve samenhang met het eindgedrag. Dit houdt in, dat een groot netto-voordeel uit het gedrag samenhangt met negatief internetbeveiligingsgedrag. Het netto-voordeel is het verschil tussen de voordelen en de niet-risicovolle kosten (zie paragraaf 1.3). De directe relatie is conform de literatuur van Compeau en Higgins (1995), hetgeen in paragraaf 1.2 staat beschreven.

De verwachte correlaties met de affectieve respons (zie paragraaf 1.3) zijn bewezen, voor de attitude en het vertrouwen. Hoge verwachtingen over de uitkomsten hangen samen met een minder negatieve attitude en een positiever vertrouwen. Hiermee is dus de tabel 1.2 bevestigd: er is een directe invloed op het eindbedrag, maar ook een indirecte, namelijk via de attitude.

De bevindingen van Shih (2006) worden hier niet bevestigd. Noch CISE, noch computervaardigheden worden significant gecorreleerd met de uitkomstverwachtingen. Het resultaat spreekt de theorie over de deels TAM tegen. De relatie met computerangst is niet significant, maar er is wel een direct effect op het eindgedrag en de attitude. In paragraaf 1.3 wordt duidelijk, dat de uitkomstverwachtingen implicaties hebben voor de risicoperceptie. Hoe negatiever de uitkomstverwachtingen, hoe minder risico mensen lopen hetgeen de beveiliging ten goede komt (zie paragraaf 1.3).

Een aanbeveling voor een volgend onderzoek is een splitsing in beide soorten uitkomstverachtingen of een grotere consistentie trachten te bewerkstelligen door een betere itemconstructie.

4.2.8 Attitude

De affectieve respons bestaat niet alleen uit attitude en vertrouwen, maar ook uit onzekerheid. De resultaten laten zien, dat attitude veel significante correlaties kent. Allereerst hangen computerangst, CISE en de uitkomstverwachtingen (cognitieve respons) samen met de attitude, wat correspondeert met de TAM (Davis, 1993). Een negatievere attitude hangt samen met meer computerangst, minder CISE en minder uitkomstverwachtingen, zoals verwacht is. Ook hangt attitude positief samen met eindgedrag, zoals is aangenomen in hoofdstuk 1. De correlatie houdt in, dat een meer negatieve attitude samenhangt met meer beveiligingsgedrag. De samenhang tussen attitude en eindgedrag is meermaals bewezen, onder andere door Davis (1993). De richting van de correlatie is op het eerste moment echter bijzonder. De gedachtegang dat onzekerheid en negatieve attitude het probleem bedreigender maken zal leiden tot een betere beveiliging, is een gangbare conslusie in de risicoperceptie. Opvallende, niet voorspelde correlaties bestaan er met angst en volharding en omgeving, waarbij de relatie met de omgeving een positieve is. Meer sociale steun, persuasie, indirecte ervaring en kwantiteit, hoe meer negatieve attitude.

4.2.9 Vertrouwen

Veel onderzoekers spreken over vertrouwen als een attitude (Corritore e.a., 2003; Pidgeon, Kasperson en Slovic, 2004). In dit onderzoek is echter gekozen voor een apart construct die samen met attitude en onzekerheid de affectieve respons van de cognitieve verwerking is. De resultaten laten zien, dat er wel degelijk een significante (negetieve) relatie bestaat met het eindgedrag. Dit houdt in, dat hoe meer vertrouwen men heeft, hoe minder beveiligingsgedrag men uitoefent. Dit lijkt een logisch gevolg bij een risico zoals het besproken is in hoofdstuk 1. Het is juist zaak om redelijk wantrouwig te zijn als het gaat om internet en de beveiliging van een computer. Waar veel sites als didid, banksites, belastingdienst en winkeliers erop hameren meer vertrouwen in het internet te hebben, hangt meer vertrouwen samen met minder beveiligingsgedrag. Ook is er een significant positieve samenhang met de onzekerheid. Hoe meer vertrouwen hoe meer onzekerheid. De richting van deze relatie is frappant te noemen, want als je ergens vertrouwen in hebt, zou er een meer zekerder gevoel moeten zijn.

Ook is er een significant verband met de omgevingsfactoren. Dit is conform de literatuur van Corritore e.a. (2003), waar de omgeving de input van het model is. In paragraaf 1.3 staat verwoord, hetgeen in het geval van totale controle, er geen vertrouwen meer nodig is (Corritore e.a., 2003), wat een relatie impliceert. Er moet wel bij worden vermeld, dat de mate van controle is gebaseerd op 27 respondenten wat een kleine groep is.

Vertrouwen is een enorm lastig construct om te meten, zeker in samenhang met een risico, wat inhoudt dat vertrouwen helemaal niet positief is. De literatuur omtrent vertrouwen is niet altijd eenduidig, dus daarom verdient het de aanbeveling zich heel erg goed in te lezen voordat zulk een construct wordt gebruikt.

4.2.10 Onzekerheid

De onzekerheid heeft een significante negatieve samenhang met het eindgedrag (r=-.20**). Dit houdt in, dat hoe onzekerder men is, hoe minder internetbeveiligingsgedrag men vertoont. Dit is tegenstrijdig met hetgeen Ropeik (2004) heeft bewezen. Zijn stelling luidt:”hoe groter de onzekerheid, hoe meer bescherming”.

De onzekerheid heeft een positieve samenhang met vertrouwen, zoals in de vorige paragraaf is besproken. Ook met attitude bestaat een positieve samenhang. Hoe onzekerder men is, hoe negatiever de attitude is. In dit licht is het opmerkelijk dat een negatieve attitude samenhangt met een sterker beveiligingsgedrag en dat een onzekerder affect samenhangt met minder beveiligingsgedrag. Met de cognitieve factoren zijn er significante verbanden, waarbij het gaat om computerangst en CISE. Hoe onzekerder de gebruiker is, hoe meer computerangst de gebruiker heeft en hoe minder CISE er is bij de gebruiker. Dit wekt de discussie weer op die uit de literatuur is gebleken. De samenhang tussen CISE, computerangst, attitude en onzekerheid is dusdanig dat het twijfels oproept over de definities en de plaats van de constructen in het onderzoeksmodel. Dit zou een goed onderwerp kunnen zijn voor een volgend onderzoek, want de discussie wordt door deze resultaten louter aangewakkerd. Met de externe stimuli is er kleine significante relatie, namelijk met angst en volharding. De samenhang tussen de nieuwheid van een risico de onzekerheid in een volgend onderzoek te bestuderen.

4.2.11 Computerbeveiligingsgedrag

Hoe het computerbeveiligingsgedrag tot stand komt is af te lezen aan figuur 3.1 en figuur 3.2. Hieruit blijkt dat attitude en CISE een belangrijke mediërende functie hebben. Het is opmerkelijk dat de negatieve gemoedstoestanden juist een positieve invloed heeft op het beveiligingsgedrag. Dit is conform de literatuur over risicoperceptie. Als men zich meer bedreigd voelt zal men zich meer beveiligen. Vanuit een leertheoretisch standpunt is dit een opmerkelijke relatie. Als men zich een gedrag heeft aangeleerd en men heeft een hoge zelfeffectiviteit, positieve uitkomstverwachtingen en een positieve attitude, zou men zich een betere beveiliging moeten aanmoeten. Men weet immers uit ervaring dat een virus zo is geïnstalleerd op de computer. Het is mogelijk dat de aanname dat computervirussen bedreigend zijn, onwaar is. In dat geval vinden mensen met voldoende kennis, CISE en attitude het helemaal niet belangrijk om zich te beschermen. Dit zou een aanbeveling kunnen zijn voor volgend onderzoek.

Literatuurlijst

Artikelen

1. Alhakami, A.S., Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and preceived benefit. *Risk analysis, 14*(6), 1085-1096.
2. Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioural Change. *Psychological Review, 84*(2), 191-215.
3. Beas, M.I., Salanova, M. (2006). Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers. *Computers in Human Behavior, 22*(6), 1043-1058.
4. Beckers, J.J., Schmidt, H.G. (2001). The structure of computer anxiety: a six-factor model. *Computers in human behavior, 17*, 35-49.
5. Beckers, J.J., Schmidt, H.G. (2003). Computer experience and computer anxiety. *Computers in human behavior,* 19(6), 785.
6. Bhattacharya, R., Devinney, T.M., Pillutla, M.M. (1998). A formal model of trust based on outcomes.*Academy of Management Review*, 23 (3), 459-472.
7. Bozionelos, N. (2001a). Computer anxiety: relationship with computer experience and prevalence. *Computers in human behavior, 17*(2), 213.
8. Bozionelos, N. (2001b). The relationship of instrumental and expressive traits with computer anxiety. *Personality and individual differences, 31*, 955-974.
9. Brosnan, M.J. (1998). The impact of computer anxiety and self-efficacy upon performance. *Journal of Computer Assisted Learning, 14*, 223-234.
10. Burkhardt, M.E., Brass, D.J. (1990). Changing patterns or Patterns of change: the effects of a change in Technology on Social Network Structure and Power. *Administrative Science Quartly, 35*(1), paginanummers.
11. Cassidy, S., Eachus, P. (2002). Developing the computer user self-efficacy (CUSE) scale: investigating the relationship between computer self-efficacy, gender and experience with computers. *J.Educational Computing Research,* 26(2), 133-153.
12. Chau, P.Y.K. (1996). An empirical assessement of a modified technological acceptance model. *Journal of Management Information Systems, 13*(3), paginanummers.
13. Cohen, F. (1984). Computer viruses, theory and experiments.
14. Compeau, D.R., Higgins, C.A. (1995). Computer Self-efficacy: development of a measure and initial test. *MIS Quarterly/ june*.
15. Corritore, C.L., Kracher B., Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*, 737-758.
16. Corritore, C.L., Marble, R.P., Widenbeck, S., Kracher, B. (2005). Measuring online trust of websites: credibility, perceived ease of use, and risk. *Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE, USA August.*
17. Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly/September,* 319-340.

18. Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989). User acceptance of computer technology: a comparisation of two theoretical models. *Management Science, 35*(8), 982-1003.
19. Davis, F.D. (1993). User acceptance of information technology: system characteristics, user perceptions ans behavioural impacts. *International Journal of Man-Machine Studies, 38,* 475-487.
20. Dishaw, M.T., Strong, D.M. (1999). Extending the technology acceptance model with task-technology fit constructs. *Information and management, 36*, 9-21.
21. Durndell, A., Haag, Z. (2002). Computer Self-efficacy, computer anxiety, attitudes towards the internet and reported experience with the internet, by gender, in an East European sample. *Computers in Human Behavior,* 18, 521-535.
22. Finucane, M.L., Alhakami, A., Slovic, P., Johnson, S.M. (2000). The Affect Heuristic in Judgements of Risks and Benefits. *Journal of Behavioral Decision Making, 13*, 1-17.
23. Fischhoff, B., Watson, S.R., Hope, C. (1984). Defining risk. *Policy sciences,* 17, 123-139.
24. Goldstein, S.B., Dudley, E.A., Erickson, C.M., Richer, N.L. (2002). Traits and computer anxiety. *Computers in Human Behavior,* 18(3), 271-284.
25. Hasan, B. (2003). The influence of specific computer experiences on computer self-efficacy beliefs. *Computers in Human Behavior,* 19, 443-450.
26. Heinssen, R.K., Glass, C.R., Knight, L.A. (1987). Assessing Computer Anxiety: Developement andValidation of the Computer Anciety Rating Scale. *Computers in Human Behaviour*, 3 (1). 49-59.
27. Hill, T., Smith, N.D., Mann, M.F. (1987). Role of efficacy expectations in predicating the decision to use advanced technologies: the case of computers. *Journal of applied psychology*, (2), 307.
28. Hinde, S. (2001). Cyberthreats: Perceptions, Reality and Protecting. *Computers and Security, 20,* 364-371.
29. Horst, M., Kuttschreuter, M., Gutteling, J.M. (2006). Perceived Usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior,* Jaargang, paginanummers
30. Igbaria, M., Iivaria, J. (1995). The effects of self-effcacy on computer usage. *Omega,* 23(6), 587-605.
31. Johnson, E.C. (2006). Security awareness: switch to better programme. *Network security, 2*, 15-18.
32. Lazar, J., Jones, A., Hackley, Schneiderman, B. (2006). Severity and impact of computer user frutration: a comparisation of student and workplace users. *Interacting with computers, 18*(2), 187-207.
33. Malhotra, Y., Galetta, D.F. (1999). Extending the Technological Acceptance Model to account for social influences : theoretical bases and empirical validation. In *Proceedings of the 32nd Hawaii International Conference on System Sciences.*

34. Marakas, G.M., George, M., Yi, M.Y., Johnson, R.D. (1998). The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research. *Information Systems Research*, 9(2), 1047-7047.
35. Maurer, M.M. (1994). Computer anxiety correlates and what they tell us: a literature review. *Computers in human behavior,* 10(3), 369-376.
36. McFarland, D.J., Hamilton, D. (2006). Adding contextual specifity to the technological acceptance model. *Computers in Human Behavior,* 22(3), 427-447.
37. Nickel, G.S., Pinto, J.N. (1986). The Computer Attitude Scale. *Computers in human behavior,* 2, 301-306.
38. Ropeik, D. (2004). The consequenses of fear. *EMBO reports,* 56-60.
39. Schumacher, P., Morahan-Martin, J. (2001). Gender, Internet and computer attitudes and experiences. *Computers in Human Behavior,* 17, 95-110.
40. Shih, H. (2006). Assessing the effects of self-efficacy and competence on individual satisfaction with computer use: an IT student perspective. *Computers in Human Behavior,* 22, 1012-1026.
41. Slovic, P. (1987). Perception of risk. *Science,* 236, 280-285.
42. Slovic, P., Finucane, M.L., Peters, E., MacGregor, D.G. (2004). Risk as analysis and risk as feelings: some thoughts about affect, reason, risk and rationality. *Risk analysis,* 24(2), 311-322.
43. Stephens, D., Creaser, C. Information Science student IT-experience and attitude toward computers: results of a five-year longitudinal study. *Information and computer science*.
44. Torkzadeh. G., van Dyke, T.P. (2001). Development and validation of an internet self-efficacy scale. *Behavior and Information Technology,* 20(4), 275-280.
45. Torkzadeh, G., van Dyke, T.P. (2002). Effects of training on internet self-efficacy and computer user attitudes. *Computers in Human Behavior,* 18, 479-494.
46. Torkzadeh, G., Chang, J.C., Demirhan, D. (2006). A contingency model of computer and internet self-efficacy. *Information and management*
47. Vlek, C.A.J. (2002). Risicologica en risicopsychologie. *Bedrijfskunde, 74*(3), 21-27.
48. Vries, B. de (2000). Uitbreken computervirussen biedt specifieke uitdaging voor communicatie. In: communicatie cases 4, 31-40.
49. Wilfong, J.D. (2006). Computer anxiety and anger: the impact of computer use, computer experience, and self-efficacy beliefs. *Computers in Human Behavior,* 22(6), 1001-1011.
50. Wilkens, L.(2001). A primer on risk. *Agbioforum, 4*(3/4), 163-172.
51. Wood, P. (2006). Yhe hacker's top five routes into the network (and how to block them). *Network security*, 2, 5-9.

Tijdschriften

52. Personal Computer Magazine, April 2006
53. Personal Computer Magazine, Augustus 2006

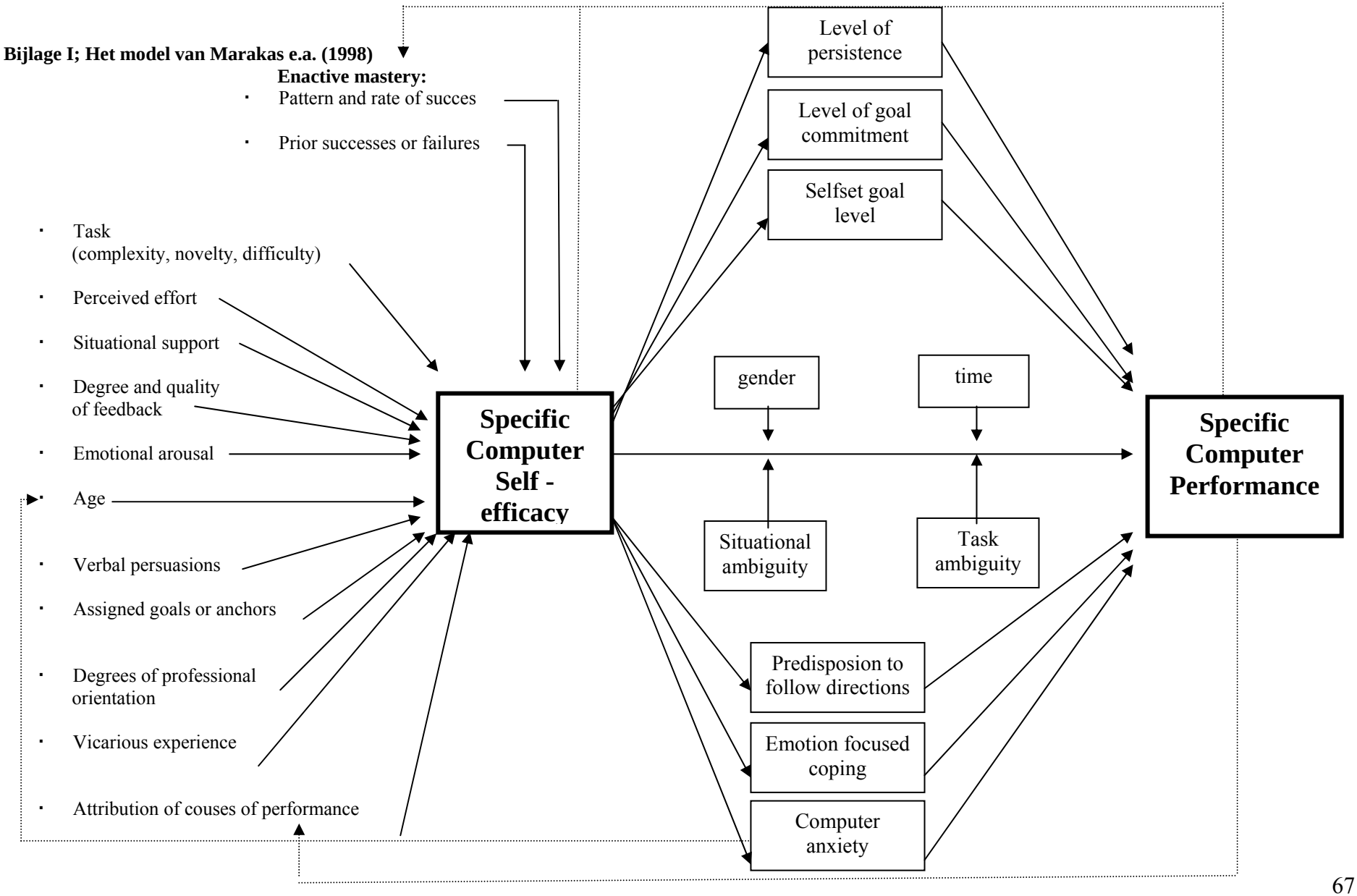
Boeken

54. Connor, M., Norman, P. (2005). *Predicting Health Behavior.* : Maidenhead, Berkshire, England: Open University Press
55. Dooley, D. (2001). *Social Research Methods.* New-Jersey: Prentice Hall, Inc.
56. Moore, D.S., McCabe, G.P. (2002). *Statistiek in de Praktijk, theorieboek.* Schoonhoven: Academic, Service.
57. Gleitman, H., Frislundm A.J., Reisberg, D. (1981). *Psychology*. New York, W.W. Norton & Company, Inc.
58. Pervin, L.A., John, O.P. (1997). *Personality in theorie and research*. Toronto, Canada: John Wiley & Sons, Inc.
59. Pidgeon, N, Kasperson, R.E., Slovic, P (2003). *The social amplification of risk*. Cambridge, Cambrigde University Press.
60. Slovic, P. (1998). *The perception of Risk.*London and Sterling: Earthscan Publications Ltd.

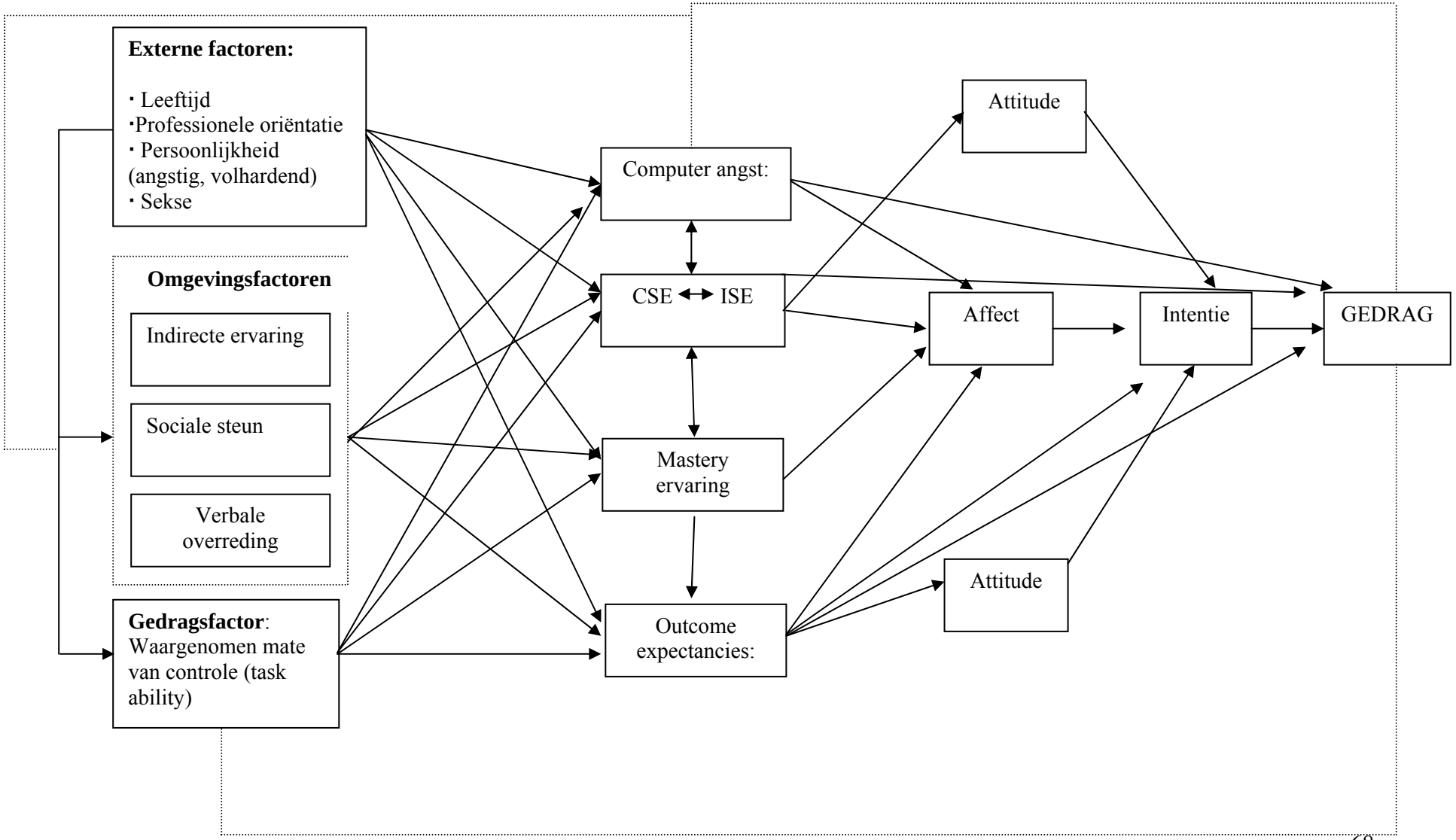
Websites

61. www.microsoft.com
62. www.xs4all.nl
63. www.digibuwust.nl
64. www.wikipedia.org
65. www.cbs.nl

Bijlage I; Het model van Marakas e.a. (1998)



Bijlage II: literatuuruitkomsten



Bijlage III; de vragenlijst

Geachte medewerk(st)er/student(e),

Hierna volgt een vragenlijst die gaat over computergedrag en computerbeveiliging. De vragenlijst telt 28 vragen verspreid over 10 pagina's. In de vragenlijst zijn antwoordinstructies vermeld. Probeert u hierbij een zo eerlijk mogelijk antwoord te geven. Als u hierbij twijfels hebt of anderszins moeite hebt met het vinden van een antwoord bedenkt u dan, dat vaak de eerste indruk de beste indruk is. De resultaten van de vragenlijst worden verwerkt in een afstudeerscriptie voor de Psychologie masterthese Veiligheid en Gezondheid, die openbaar zal zijn. Uw anonimiteit wordt wel te allen tijde gewaarborgd.
Mocht u vragen hebben kunt u altijd mailen naar m.k.vandijk@student.utwente.nl
Hartelijk dank voor uw tijd en moeite!

Marike van Dijk

Algemene Vragen

V1 Wat is uw leeftijd?
- V1_1 Jonger dan 18
- V1_2 18 t/m 25
- V1_3 6 t/m 35
- V1_4 6 t/m 45
- V1_5 6 t/m 55
- V1_6 6 t/m 65
- V1_7 ouder dan 65

V2 Wat is uw geslacht
- V2_1 Man
- V2_2 Vrouw

V3 Wat is uw hoogst genoten opleiding?
- V3_1 LBO
- V3_2 MAVO
- V3_3 MBO
- V3_4 MBO+
- V3_5 HAVO
- V3_6 HBO
- V3_7 HBO+
- V3_8 VWO
- V3_9 WO
- V3_10 WO+

V4 Hoe bent u verbonden aan de faculteit gedragswetenschappen?
- V4_1 Student
- V4_2 In dienst van de UT

Internet

Komende vragen betreffen uw verbinding met het internet en uw gebruik van het internet thuis. Met een Personal Computer wordt de computer bedoeld waarmee u de administratie, de tekstverwerking doet en het internet gebruikt.

V5 Hoeveel Personal Computers telt uw huishouden?
V5_1
V5_2
V5_3
V5_4
V5_5

V6 Maakt u thuis gebruik van een draadloze internetverbinding?
V6_1 Ja
V6_2 Nee

V7 Heeft u thuis een draadloos netwerk?
V7_1 Ja
V7_2 Nee

V8 Hoevaak maakt u gebruik van het internet via een laptop?
V8_1 Nooit
V8_2 Een enkele keer
V8_3 Regelmatig
V8_4 Altijd

V9 Hoeveel uren brengt u thuis op het internet (online) door?
V9_1 <-10 uren per week
V9_2 11-20 uren uur per week
V9_3 21-30 uren per week
V9_4 31-40 uren per week
V9_5 41-50 uren per week
V9_6 >50 uren per week

V10 Waar gebruikt u het internet het meeste voor? U kunt uit de onderstaande mogelijkheden de vijf meest gebruikte internetfuncties uitzoeken en deze rangschikken van 5 (meeste gebruikt) tot 1.
V10_1_1-V10_1_5 Ontspanning, recreatie
V10_2_1-V10_2_5 Informatie zoeken
V10_3_1-V10_3_5 Informatie-opslag
V10_4_1-V10_4_5 Chatten, bijvoorbeeld MSN
V10_5_1-V10_5_5 E-mail
V10_6 _1-V10_6_5 Multimedia (tv, radio)
V10_7 _1-V10_7_5 Downloaden van films en muziek
V10_8_1-V10_8_5 Eigen website
V10_9_1-V10_9_5 Administratie zoals online bankieren belasting doen of digid gebruik
V10_10_1-V10_10_5 Door middel van creditcard aankopen doen

Gebruik van eventuele kinderen

Onderstaande vragen gaan over uw (eventuele) kinderen en hun internetgebruik.

V11 Hoeveel kinderen heeft u?
V11_1 Geen → ga naar vraag 18
V11_2 1
V11_3 2
V11_4

V11_5 meer dan 3

V12 Hoeveel tijd brengen uw kinderen thuis gemiddeld achter de computer door?
V12_1 <5 uur per week
V12_2 5-10 uur per week
V12_3 11-15 uur per week
V12_4 16-20 uur per week
V12_5 21-25 uur per week
V12_6 >25 uur per week

V13 Waar, denkt u, gebruiken uw kinderen het internet het meeste voor? U kunt uit de onderstaande mogelijkheden de vijf beste internetfuncties rangschikken van 5 (meeste gebruikt) tot 1.

V13_1_1-V13_1_5	On-line spelletjes
V13_2_1-V13_2_5	Informatie zoeken, bijvoorbeeld via Google
V13_3_1-V13_3_5	Chatten, bijvoorbeeld MSN
V13_4_1-V13_4_5	E-mail
V13_5_1-V13_5_5	Multimedia (tv, radio)
V13_6_1-V13_6_5	Downloaden van films en muziek
V13_7_1-V13_7_5	Eigen website
V13_8_1-V13_8_5	Aankopen doen
V13_9_1-V13_9_5	Educatieve programma's

V14 In de onderstaande stellingen wordt er naar uw mening gevraagd. U kunt uit zes antwoorden kiezen welke het beste van toepassing is op uw situatie.

V14a Hoeveel toezicht heeft u op het downloadgedrag van uw kinderen?
V14a_1 Erg Veel
V14a_2 Veel
V14a_3 Redelijk Veel
V14a_4 Redelijk Weinig
V14a_5 Weinig
V14a_6 Nooit

V14b In hoeverre heeft u afspraken gemaakt met uw kinderen over het downloaden van programma's?
V14b_1 Erg Veel
V14b_2 Veel
V14b_3 Redelijk Veel
V14b_4 Redelijk Weinig
V14b_5 Weinig
V14b_6 Nooit

V14c In hoeverre heeft u afspraken gemaakt met uw kinderen over het downloaden van bestanden?
V14c_1 Erg veel
V14c_2 Veel
V14c_3 Redelijk Veel
V14c_4 Redelijk Weinig
V14c_5 Weinig
V14c_6 Nooit

V14d In hoeverre bent u angstig dat uw Personal Computer door toedoen van uw kinderen wordt besmet met een virus?

V14d_1 Erg veel
V14d_2 Veel
V14d_3 Redelijk Veel
V14d_4 Redelijk Weinig
V14d_5 Weinig
V14d_6 Nooit

Internetproblemen

De volgende twee vragen betreffen de mogelijke problemen die u heeft gehad met het internet. Met een computerexpert wordt een deskundige vriend, maar ook een helpdesk bedoeld.

V15 Hoe vaak beroept u zich op een computerdeskundige als er problemen met uw Personal Computer zijn?

V15_1 Nooit
V15_2 Ongeveer eens in het jaar
V15_3 Ongeveer 6 keer in het jaar
V15_4 Ongeveer elke maand
V15_5 Ongeveer twee keer in de maand
V15_6 Eén of meerdere keren per week

V16 Voor welke problemen met de Personal Computer beroept u zich op een computerdeskundige? Graag maximaal 4 antwoorden aankruizen.

V16_1 Internetverbinding
V16_2 Netwerkverbinding
V16_3 Trage computer
V16_4 Als een programma het niet meer doet
V16_5 Als ik een bepaald programma wil downloaden
V16_6 Als ik software wil lenen
V16_7 Computerbeveiliging
V16_8 Computerproblemen op de UT
V16_9 Password of account doet het niet meer
V16_10 Netwerkproblemen
V16_11 Nooit
V16_12 Anders, namelijk…

V17. Hierna wordt er gevraagd naar uw mening in de vorm van stellingen. Deze stellingen hebben betrekking op de manier hoe u op uw Personal Computer met internetbeveiliging om gaat. Er zijn zes antwoordmogelijkheden, waarvan u er één kunt kiezen.

V17a Er is altijd iemand op wie ik kan terugvallen als het gaat om computerbeveiliging.

V17a_1 Helemaal Oneens
V17a_2 Oneens
V17a_3 Redelijk Oneens
V17a_4 Redelijk Eens
V17a_5 Eens
V17a_6 Helemaal Eens

V17b Ik open nooit een bijlage waar ik twijfel over heb.

V17b_1 Helemaal Oneens
V17b_2 Oneens

V17b_3 Redelijk Oneens
V17b_4 Redelijk Eens
V17b_5 Eens
V17b_6 Helemaal Eens

V16_c Ik open alleen een bijlage waarvan ik weet dat het naar mij verstuurd is
V17c_1 Helemaal Oneens
V17c_2 Oneens
V17c_3 Redelijk Oneens
V17c_4 Redelijk Eens
V17c_5 Eens
V17c_6 Helemaal Eens

V16d Ik klik nooit door op een e-mail-link van een officiële instantie
V17d_1 Helemaal Oneens
V17d_2 Oneens
V17d_3 Redelijk Oneens
V17d_4 Redelijk Eens
V17d_5 Eens
V17d_6 Helemaal Eens

V17e Ik zorg ervoor dat mijn computer een goede antivirus en firewall heeft
V17e_1 Helemaal Oneens
V17e_2 Oneens
V17e_3 Redelijk Oneens
V17e_4 Redelijk Eens
V17e_5 Eens
V17e_6 Helemaal Eens

V17f Ik sta huiverig tegenover het gebruik van programma's waarvan ik weet dat ze virusgevoelig zijn.
V17f_1 Helemaal Oneens
V17f_2 Oneens
V17f_3 Redelijk Oneens
V17f_4 Redelijk Eens
V17f_5 Eens
V17f_6 Helemaal Eens

V17g Ik maak regelmatig backups.
V17g_1 Helemaal Oneens
V17g_2 Oneens
V17g_3 Redelijk Oneens
V17g_4 Redelijk Eens
V17g_5 Eens
V17g_6 Helemaal Eens

V17h Ik download alleen van sites waarvan ik zeker weet dat ze veilig zijn.
V17h_1 Helemaal Oneens
V17h_2 Oneens
V17h_3 Redelijk Oneens
V17h_4 Redelijk Eens
V17h_5 Eens

V17h_6 Helemaal Eens

Affect

V18 De onderstaande stellingen hebben betrekking op uw gevoel over het internet thuis, tenzij het anders aangegeven wordt.

V18a Het internet met al zijn risico's geeft me een oncomfortabel gevoel.
- V18a_1 Helemaal Oneens
- V18a_2 Oneens
- V18a_3 Redelijk Oneens
- V18a_4 Redelijk Eens
- V18a_5 Eens
- V18a_6 Helemaal Eens

V18b De mogelijke internetrisico´s benauwen mij.
- V18b_1 Helemaal Oneens
- V18b_2 Oneens
- V18b_3 Redelijk Oneens
- V18b_4 Redelijk Eens
- V18b_5 Eens
- V18b_6 Helemaal Eens

V18c De mogelijke internetrisico's frustreren mij.
- V18c_1 Helemaal Oneens
- V18c_2 Oneens
- V18c_3 Redelijk Oneens
- V18c_4 Redelijk Eens
- V18c_5 Eens
- V18c_6 Helemaal Eens

V18d Het internet is verantwoordelijk voor veel leuke dingen.
- V18d_1 Helemaal Oneens
- V18d_2 Oneens
- V18d_3 Redelijk Oneens
- V18d_4 Redelijk Eens
- V18d_5 Eens
- V18d_6 Helemaal Eens

V18e Het internet is verantwoordelijk voor veel slechte dingen.
- V18e_1 Helemaal Oneens
- V18e_2 Oneens
- V18e_3 Redelijk Oneens
- V18e_4 Redelijk Eens
- V18e_5 Eens
- V18e_6 Helemaal Eens

V18f De complexiteit van de methoden om mijn computer te beveiligen schrikt mij af.
- V18f_1 Helemaal Oneens
- V18f_2 Oneens
- V18f_3 Redelijk Oneens

V18f_4 Redelijk Eens
V18f_5 Eens
V18f_6 Helemaal Eens

V19.

V19a Ik geloof dat anderen mij altijd eerlijk en integer behandelen via het internet.
V19a_1 Helemaal Oneens
V19a_2 Oneens
V19a_3 Redelijk Oneens
V19a_4 Redelijk Eens
V19a_5 Eens
V19a_6 Helemaal Eens

V19b Ik ken de sites met een onveilige reputatie.
V19b_1 Helemaal Oneens
V19b_2 Oneens
V19b_3 Redelijk Oneens
V19b_4 Redelijk Eens
V19b_5 Eens
V19b_6 Helemaal Eens

V19c Een link in een e-mail is altijd te vertrouwen.
V19c_1 Helemaal Oneens
V19c_2 Oneens
V19c_3 Redelijk Oneens
V19c_4 Redelijk Eens
V19c_5 Eens
V19c_6 Helemaal Eens

V19d Antivirus aanbieders hebben altijd het beste met mij voor.
V19d_1 Helemaal Oneens
V19d_2 Oneens
V19d_3 Redelijk Oneens
V19d_4 Redelijk Eens
V19d_5 Eens
V19d_6 Helemaal Eens

V19e De computerexpert (helpdesk of deskundige vriend) heeft altijd gelijk.
V19e_1 Helemaal Oneens
V19e_2 Oneens
V19e_3 Redelijk Oneens
V19e_4 Redelijk Eens
V19e_5 Eens
V19e_6 Helemaal Eens

V19f Ik sta nauwelijks stil bij internetrisico's, omdat ze mij niet overkomen.
V19f_1 Helemaal Oneens
V19f_2 Oneens
V19f_3 Redelijk Oneens
V19f_4 Redelijk Eens
V19f_5 Eens

V19f_6 Helemaal Eens

V19g Op een UT-computer hoef ik me niet druk te maken over virussen.
V19g_1 Helemaal Oneens
V19g_2 Oneens
V19g_3 Redelijk Oneens
V19g_4 Redelijk Eens
V19g_5 Eens
V19g_6 Helemaal Eens

Ervaring

20.
Als ik mijzelf een rapportcijfer moest geven voor computerdeskundigheid in het algemeen dan zou ik mijzelf het volgende cijfer geven:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

De volgende stellingen gaan over activiteiten en eerdere ervaring ermee met betrekking tot het internet.
V21. Onderstaande vragen gaan over de voor-en nadelen van het internet.
V21a Als informatie erg moeilijk op een andere manier te verkrijgen is, ben ik bereid om een internetrisico te nemen.
V21a_1Helemaal Oneens
V21a_2 Oneens
V21a_3 Redelijk Oneens
V21a_4 Redelijk Eens
V21a_5 Eens
V21a_6 Helemaal Eens

V21b Ik chat graag via de computer, ook al weet ik dat het beveiligingsrisico's met zich meebrengt.
V21b_1 Helemaal Oneens
V21b_2 Oneens
V21b_3 Redelijk Oneens
V21b_4 Redelijk Eens
V21b_5 Eens
V21b_6 Helemaal Eens

V21c Ik haal muziek gratis van het internet, ook al weet ik dat het meer risico's met zich meebrengt.
V21c_1Helemaal Oneens
V21c_2 Oneens
V21c_3 Redelijk Oneens
V21c_4 Redelijk Eens
V21c_5 Eens
V21c_6 Helemaal Eens

V21d Ik heb eenvoudig te onthouden wachtwoorden.
V21d_1 Helemaal Oneens
V21d_2 Oneens
V21d_3 Redelijk Oneens
V21d_4 Redelijk Eens

V21d_5 Eens
V21d_6 Helemaal Eens

V21e Een backup maken laat ik wel eens achterwege.
V21e_1 Helemaal Oneens
V21e_2 Oneens
V21e_3 Redelijk Oneens
V21e_4 Redelijk Eens
V21e_5 Eens
V21e_6 Helemaal Eens

V21f Ik maak me druk om de beveiliging van mijn computer.
V21f_1 Helemaal Oneens
V21f_2 Oneens
V21f_3 Redelijk Oneens
V21f_4 Redelijk Eens
V21f_5 Eens
V21f_6 Helemaal Eens

V22. Onderstaande stellingen hebben te maken met ervaring.
V22a Ik heb cursussen gedaan om internetbeveiliging onder de knie te krijgen.
V22a_1 Helemaal Oneens
V22a_2 Oneens
V22a_3 Redelijk Oneens
V22a_4 Redelijk Eens
V22a_5 Eens
V22a_6 Helemaal Eens

V22b Ik besef dat mijn computer gebruikt kan worden door anderen bijvoorbeeld voor virusverspreiding.
V22b_1 Helemaal Oneens
V22b_2 Oneens
V22b_3 Redelijk Oneens
V22b_4 Redelijk Eens
V22b_5 Eens
V22b_6 Helemaal Eens

V22c Mijn computer is besmet geraakt door onbetrouwbare sites als Kazaa, Limewire of MSN.
V22c_1 Helemaal Oneens
V22c_2 Oneens
V22c_3 Redelijk Oneens
V22c_4 Redelijk Eens
V22c_5 Eens
V22c_6 Helemaal Eens

V22d Ik ben wel eens de dupe geweest van internetoplichterij.
V22d_1 Helemaal Oneens
V22d_2 Oneens
V22d_3 Redelijk Oneens
V22d_4 Redelijk Eens
V22d_5 Eens
V22d_6 Helemaal Eens

V23. Onderstaande stellingen hebben betrekking op uw deskundigheid aangaande computeractiviteiten.

V23a Als er problemen zijn met de beveiliging van mijn computer kan ik ze doorgaans zelf oplossen.

V23a_1 Helemaal Oneens
V23a_2 Oneens
V23a_3 Redelijk Oneens
V23a_4 Redelijk Eens
V23a_5 Eens
V23a_6 Helemaal Eens

V23b Antivirusprogramma's zijn eenvoudig uit te zoeken, te downloaden en te updaten

V23b_1 Helemaal Oneens
V23b_2 Oneens
V23b_3 Redelijk Oneens
V23b_4 Redelijk Eens
V23b_5 Eens
V23b_6 Helemaal Eens

V23c Ik vind het moeilijk om computers te laten doen wat ik wil dat ze doen.

V23c_1 Helemaal Oneens
V23c_2 Oneens
V23c_3 Redelijk Oneens
V23c_4 Redelijk Eens
V23c_5 Eens
V23c_6 Helemaal Eens

V23d Ik vind het eenvoudig om een backup te maken.

V23d_1 Helemaal Oneens
V23d_2 Oneens
V23d_3 Redelijk Oneens
V23d_4 Redelijk Eens
V23d_5 Eens
V23d_6 Helemaal Eens

V23e Als ik een computer gebruik gebeuren er soms dingen die ik niet kan verklaren.

V23e_1 Helemaal Oneens
V23e_2 Oneens
V23e_3 Redelijk Oneens
V23e_4 Redelijk Eens
V23e_5 Eens
V23e_6 Helemaal Eens

V23f Ik voel me zelfverzekerd over mijn computerbeveiliging.

V23f_1 Helemaal Oneens
V23f_2 Oneens
V23f_3 Redelijk Oneens
V23f_4 Redelijk Eens
V23f_5 Eens
V23f_6 Helemaal Eens

Zelfevaluatie

V24. Geef uzelf een rapportcijfer (van 1 tot 10) voor de volgende handelingen:

V24a_1-10 maken van backups.
V24b_1-10 het uitzoeken van een antivirusprogramma en firewall.
V24c_1-10 het instaleren van een antivirusprogramma en firewall.
V24d_1-10 het beoordelen van een bijlage in een e-mail.
V24f_1-10het beoordelen van de betrouwbaarheid van sites.

Omgeving

V25. Onderstaande stellingen betreffen de eventuele ondersteuning van uw omgeving.

V25a Anderen sporen mij aan om aan de computerbeveiliging te denken.
V25a_1Helemaal Oneens
V25a_2 Oneens
V25a_3 Redelijk Oneens
V25a_4 Redelijk Eens
V25a_5 Eens
V25a_6 Helemaal Eens

V25b Er is iemand in mijn vriendenkring of bij de helpdesk die ik altijd iets kan vragen over computerbeveiliging.
V25b_1Helemaal Oneens
V25b_2 Oneens
V25b_3 Redelijk Oneens
V25b_4 Redelijk Eens
V25b_5 Eens
V25b_6 Helemaal Eens

V25c Als een bekende advies geeft over de beveiliging van mijn PC, dan volg ik dat altijd op.
V25c_1Helemaal Oneens
V25c_2 Oneens
V25c_3 Redelijk Oneens
V25c_4 Redelijk Eens
V25c_5 Eens
V25c_6 Helemaal Eens

V25d Ik installeer alleen de antivirusprogramma's waarvan ik weet dat ze bij anderen ook effectief zijn.
V25d_1Helemaal Oneens
V25d_2 Oneens
V25d_3 Redelijk Oneens
V25d_4 Redelijk Eens
V25d_5 Eens
V25d_6 Helemaal Eens

V25e Ik heb Kazaa op de computer, omdat iedereen dat op de computer heeft.

V25e_1 Helemaal Oneens
V25e_2 Oneens
V25e_3 Redelijk Oneens
V25e_4 Redelijk Eens
V25e_5 Eens
V25e_6 Helemaal Eens

V25f Alles wat ik op de UT leer over computerbeveiliging, pas ik thuis toe.
V25f_1 Helemaal Oneens
V25f_2 Oneens
V25f_3 Redelijk Oneens
V25f_4 Redelijk Eens
V25f_5 Eens
V25f_6 Helemaal Eens

V26. De volgende stellingen betreffen uw gedachten over de veiligheid van de computer en het internet.

V26a Het is beangstigend dat de computer grote hoeveelheden informatie kan verwijderen door een druk op de verkeerde knop.
V26a_1 Helemaal Oneens
V26a_2 Oneens
V26a_3 Redelijk Oneens
V26a_4 Redelijk Eens
V26a_5 Eens
V26a_6 Helemaal Eens

V26b Ik twijfel wel eens aan internetbankieren, omdat ik bang ben dat het niet genoeg beveiligd is.
V26b_1 Helemaal Oneens
V26b_2 Oneens
V26b_3 Redelijk Oneens
V26b_4 Redelijk Eens
V26b_5 Eens
V26b_6 Helemaal Eens

V26c Ik voel me machteloos als ik aan de gevaren van het internet denk.
V26c_1 Helemaal Oneens
V26c_2 Oneens
V26c_3 Redelijk Oneens
V26c_4 Redelijk Eens
V26c_5 Eens
V26c_6 Helemaal Eens

V26d Ik mijd computers of het internet wel eens, omdat ik bang ben dat iemand anders informatie van mijn PC kan halen.
V26d_1 Helemaal Oneens
V26d_2 Oneens
V26d_3 Redelijk Oneens
V26d_4 Redelijk Eens
V26d_5 Eens

V26d_6 Helemaal Eens

V26e Ik prefereer het handmatig verwerken en -werven van informatie omdat ik dat veiliger vind.
V26e_1 Helemaal Oneens
V26e_2 Oneens
V26e_3 Redelijk Oneens
V26e_4 Redelijk Eens
V26e_5 Eens
V26e_6 Helemaal Eens

V26f Het leren beveiligen van een computer is net als het aanleren van een andere nieuwe vaardigheid: hoe meer er wordt geoefend, hoe beter iemand wordt.
V26f_1 Helemaal Oneens
V26f_2 Oneens
V26f_3 Redelijk Oneens
V26f_4 Redelijk Eens
V26f_5 Eens
V26f_6 Helemaal Eens

Persoonlijkheid

V27. De volgende stellingen gaan over het computergebruik en het internetgebruik in het algemeen.

V27a Ik weet precies hoe het internet werkt.
V27a_1 Helemaal Oneens
V27a_2 Oneens
V27a_3 Redelijk Oneens
V27a_4 Redelijk Eens
V27a_5 Eens
V27a_6 Helemaal Eens

V27b Ik denk dat ik een computer nooit volledig zal begrijpen.
V27b_1 Helemaal Oneens
V27b_2 Oneens
V27b_3 Redelijk Oneens
V27b_4 Redelijk Eens
V27b_5 Eens
V27b_6 Helemaal Eens

V27c Ik denk dat ik computervirussen nooit helemaal onder de knie krijg.
V27c_1 Helemaal Oneens
V27c_2 Oneens
V27c_3 Redelijk Oneens
V27c_4 Redelijk Eens
V27c_5 Eens
V27c_6 Helemaal Eens

V27d Als er een onzekere site is die ik toch wil bekijken, doe ik dat op de UT.
V27d_1 Helemaal Oneens
V27d_2 Oneens

V27d_3 Redelijk Oneens
V27d_4 Redelijk Eens
V27d_5 Eens
V27d_6 Helemaal Eens

V27e De veiligheid van een Personal Computer ligt geheel in eigen handen.
V27e_1 Helemaal Oneens
V27e_2 Oneens
V27e_3 Redelijk Oneens
V27e_4 Redelijk Eens
V27e_5 Eens
V27e_6 Helemaal Eens

V28 Deze laatste vragen gaan over uw persoonlijkheid in het algemeen.

V28a Ik voel me vaak gespannen en zenuwachtig.
V28a_1 Helemaal Oneens
V28a_2 Oneens
V28a_3 Redelijk Oneens
V28a_4 Redelijk Eens
V28a_5 Eens
V28a_6 Helemaal Eens

V28b Ik maak me vaak zorgen over dingen die mis zouden kunnen gaan.
V28b_1 Helemaal Oneens
V28b_2 Oneens
V28b_3 Redelijk Oneens
V28b_4 Redelijk Eens
V28b_5 Eens
V28b_6 Helemaal Eens

V28c Ik voel me vaak hulpeloos en wil dan graag dat iemand mijn problemen oplost.
V28c_1 Helemaal Oneens
V28c_2 Oneens
V28c_3 Redelijk Oneens
V28c_4 Redelijk Eens
V28c_5 Eens
V28c_6 Helemaal Eens

V28d Ik heb mezelf tamelijk goed in de hand in een crisis.
V28d_1 Helemaal Oneens
V28d_2 Oneens
V28d_3 Redelijk Oneens
V28d_4 Redelijk Eens
V28d_5 Eens
V28d_6 Helemaal Eens

V28e Ik heb veel zelfdiscipline.
V28e_1 Helemaal Oneens
V28e_2 Oneens

V28e_3 Redelijk Oneens
V28e_4 Redelijk Eens
V28e_5 Eens
V28e_6 Helemaal Eens

V28f Wanneer een project te moeilijk wordt, ben ik geneigd met iets anders te beginnen.
V28f_1 Helemaal Oneens
V28f_2 Oneens
V28f_3 Redelijk Oneens
V28f_4 Redelijk Eens
V28f_5 Eens
V28f_6 Helemaal Eens

Hartelijk dank voor het invullen. Mocht u geïnteresseerd zijn in de gegevens kunt u een mail sturen naar m.k.vandijk@student.utwente.nl. Voor de studenten worden de resultaten op teletop gezet.

Marike van Dijk

Bijlage 4; Frequenties

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Variance
V1	184	4	2	6	2,89	1,151	1,326
V2	184	1	1	2	1,60	,491	,241
V3	184	9	1	10	8,38	1,444	2,084
V4	184	1	1	2	1,41	,493	,243
V5	184	3	1	4	2,48	1,126	1,267
V6	184	1	1	2	1,46	,500	,250
V7	184	1	1	2	1,40	,492	,242
V8	184	4	1	5	2,90	1,387	1,925
V9	184	5	1	6	2,38	1,274	1,624
V10_1	131	4	1	5	2,82	1,375	1,889
V10_2	160	4	1	5	3,55	1,212	1,469
V10_3	39	4	1	5	2,46	1,232	1,518
V10_4	90	4	1	5	3,09	1,363	1,857
V10_5	164	4	1	5	4,01	1,231	1,515
V10_6	36	4	1	5	2,69	1,369	1,875
V10_7	88	4	1	5	2,47	1,241	1,539
V10_8	33	4	1	5	2,36	1,270	1,614
V10_9	132	4	1	5	2,48	1,195	1,427
V10_10	46	4	1	5	1,57	1,003	1,007
V11	184	4	0	4	,30	,765	,584
V12	34	3	1	4	2,15	1,048	1,099
V13_1	22	4	1	5	3,55	1,625	2,641
V13_2	20	4	1	5	3,25	1,209	1,461
V13_3	17	4	1	5	3,65	1,618	2,618
V13_4	10	3	2	5	3,50	,972	,944
V13_5	6	4	1	5	3,00	1,414	2,000
V13_6	15	4	1	5	2,67	,900	,810
V13_7	3	2	2	4	2,67	1,155	1,333
V13_8	0						
V13_9	13	4	1	5	2,38	1,710	2,923
V14a	27	5	0	5	2,74	1,655	2,738
V14b	27	5	0	5	2,48	1,847	3,413
V14c	26	5	0	5	2,27	1,733	3,005
V14dR	27	5	0	5	1,96	1,556	2,422
V15	184	4	0	4	1,02	,911	,830
Valid N (listwise)	0						

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
F16	0					
V17a	184	0	5	3,32	1,414	2,000
V17b	184	0	5	3,99	1,121	1,257
V17c	184	0	5	3,33	1,357	1,840
V17d	184	0	5	1,64	1,212	1,468
V17e	183	0	5	3,86	1,272	1,617
V17f	184	0	5	2,91	1,348	1,818
V17g	183	0	5	2,57	1,488	2,214
V17h	183	0	5	2,84	1,260	1,588
V18a	174	0	5	,92	1,017	1,034
V18b	174	0	4	1,05	,939	,882
V18c	174	0	5	1,38	1,265	1,601
V18d	174	0	5	3,87	,871	,758
V18e	174	0	5	2,80	1,258	1,584
V18f	174	0	5	1,74	1,347	1,814
V19a	174	0	5	1,93	1,226	1,503
V19b	174	0	5	2,08	1,209	1,462
V19c	174	0	5	,63	,715	,511
V19d	174	0	5	1,81	1,180	1,392
V19e	174	0	5	2,11	1,267	1,605
V19f	174	0	5	1,98	1,240	1,537
V19g	174	0	5	2,28	1,384	1,914
V20	171	2	10	6,75	1,435	2,060
V21a	171	0	5	3,18	1,110	1,232
V21b	171	0	5	2,29	1,647	2,714
C21c	171	0	5	2,80	1,647	2,713
C21d	171	0	5	2,35	1,445	2,088
V21e	171	0	5	3,05	1,307	1,709
V21fR	171	0	5	2,79	1,242	1,544
Valid N (listwise)	0					

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Variance
V22a	171	0	4	,39	,739	,546
V22b	171	0	5	3,77	1,118	1,251
V22c	171	0	5	1,36	1,490	2,221
V22d	171	0	5	,67	1,011	1,022
V23a	171	0	5	2,89	1,419	2,012
V23b	171	0	5	2,99	1,328	1,765
V23cR	171	0	5	3,58	1,116	1,245
V23d	171	0	5	3,57	1,328	1,765
V23eR	171	0	5	2,67	1,363	1,859
V23f	171	0	5	3,19	1,180	1,392
V24a	171	1	10	5,56	2,610	6,812
V24b	171	1	10	6,16	2,285	5,220
V24c	171	1	10	6,64	2,333	5,444
V24d	171	3	10	7,73	1,467	2,151
V24e	171	2	10	7,02	1,545	2,388
V25a	168	0	5	2,27	1,446	2,092
V25b	168	0	5	3,68	1,273	1,621
V25c	168	0	5	2,61	1,218	1,484
V25d	168	0	5	3,08	1,278	1,634
V25e	168	0	5	,39	,804	,646
V25f	168	0	5	1,92	1,364	1,861
V26a	168	0	5	2,09	1,447	2,094
V26b	168	0	5	1,48	1,248	1,556
V26c	168	0	5	1,19	1,055	1,113
V26d	168	0	4	,80	,930	,865
V26e	168	0	4	,76	,856	,733
V26fR	167	0	5	1,54	1,118	1,249
V27aR	167	0	5	2,85	1,170	1,369
V27b	167	0	5	2,81	1,366	1,867
V27c	167	0	5	2,82	1,277	1,630
V27d	167	0	5	1,47	1,293	1,672
V27e	167	0	5	2,93	1,198	1,435
V28a	167	0	5	1,20	1,073	1,151
V28b	167	0	5	1,76	1,276	1,629
V28c	166	0	4	1,11	,981	,963
V28dR	167	0	5	1,47	,805	,648
V28eR	167	0	5	1,69	1,150	1,322
V28f	167	0	5	1,71	1,132	1,281
Valid N (listwise)	165					

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Vraag 28	166	0	18	7,53	3,796
Vraag 15, 17a, 25	168	1	29	16,61	4,988
Vraag 26	168	0	14	5,71	3,373
Vraag 23	171	1	26	16,23	4,838
Vraag 21	171	0	20	11,24	3,939
Attitude	167	3	33	13,89	5,166
Vraag 19	174	0	17	8,84	3,442
Gedragfactoren	181	6	26	17,17	4,044
Vraag 14 en 9	26	1	20	9,58	5,261
Onzekerheid	167	2	21	10,51	3,742
Valid N (listwise)	26				